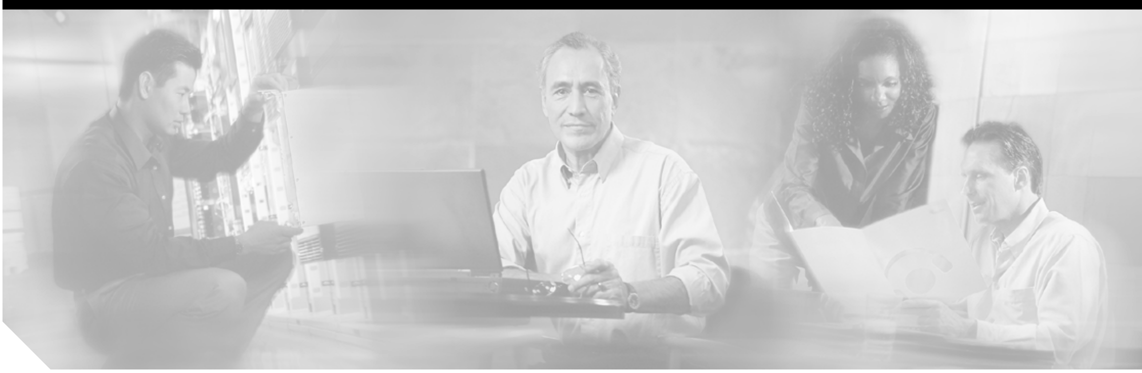
CISCO SYSTEMS



Cisco 12006 and Cisco 12406 Router Installation and Configuration Guide

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-11497-03

CONTENTS

Preface

Audience

The *Cisco 12006 and Cisco 12406 Router Installation and Configuration Guide* is written for hardware installers and system administrators of Cisco routers.

This publication assumes that the user has a substantial background in installing and configuring router and switch-based hardware. The reader should also be familiar with electronic circuitry and wiring practices, and have experience as an electronic or electromechanical technician.

Purpose

This installation and configuration guide contains procedures for installing the router hardware, creating a basic startup configuration file, and powering on the router for the first time.

Organization

The *Cisco 12006 and Cisco 12406 Router Installation and Configuration Guide* contains the following chapters, appendix, and index.

- Chapter 1, "Product Overview"—Presents a high-level system overview and physical description of the major components of Cisco 12006 and Cisco 12406 Routers, including the power and cooling systems, Gigabit Route Processor (GRP), Performance Route Processor (PRP), clock and scheduler cards (CSC), switch fabric cards (SFC), and alarm cards, and gives a functional overview.
- Chapter 2, "Preparing for Installation"—Discusses safety, site requirements for power, environmental safety, cabling, rack-mounting, electrostatic discharge (ESD), unpacking, site log, and site preparation checklist.
- Chapter 3, "Installing the Router"—Gives the procedures for the initial installation and setup of Cisco 12006 and Cisco 12406 Routers.
- Chapter 4, "Troubleshooting the Installation"—Explains how to identify and solve problems that might occur during installation.
- Chapter 5, "Field Diagnostics for the Cisco 12000 Series Router"—Describes how to load and run the field diagnostics for the Cisco 12000 Series Internet Router.
- Chapter 6, "Maintaining the Router"—Explains safety at the field-replaceable unit (FRU) level, removal and replacement procedures for field-replaceable units and assemblies, and associated procedures to troubleshoot and verify FRU and device operation.
- Appendix A, "Technical Specifications"—Provides the technical specifications and connector cable specifications for Cisco 12006 and Cisco 12406 Routers.
- Index

Document Conventions

This publication uses the following conventions:

- Ctrl- represents the key labeled *Control*. For example, the key combination **Ctrl-z** means hold down the **Control** key while you press the **z** key.

Command descriptions use these conventions:

- Examples that contain system prompts denote interactive sessions, indicating the commands that you should enter at the prompt. The system prompt indicates the current level of the EXEC command interpreter.

  For example, the prompt `router>` indicates that you should be at the *user* level, and the prompt `router#` indicates that you should be at the *privileged* level. Access to the privileged level usually requires a password. Refer to the related software configuration and reference documentation for additional information.
- Commands and keywords are in **boldface** font.
- Arguments for which you supply values are in *italic* font.
- Elements in square brackets ([ ]) are optional.
- Alternative but required keywords are grouped in braces ({ }) and separated by vertical bars (|).

Examples use these conventions:

- Terminal sessions and sample console screen displays are in `screen` font.
- Information you enter is in **`boldface screen`** font.
- Nonprinting characters, such as passwords, are in angle brackets (< >).
- Default responses to system prompts are in square brackets ([ ]).
- Exclamation points (!) at the beginning of a line indicate a comment line.

Caution Means *reader be careful*. You are capable of doing something that might result in equipment damage or loss of data.

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning **This warning symbol means *danger*. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Cisco will continue to support documentation orders using the Ordering tool:

- Registered Cisco.com users (Cisco direct customers) can order documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Instructions for ordering documentation using the Ordering tool are at this URL:

  http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support and Documentation Website

The Cisco Technical Support andDocumentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help

solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

http://www.cisco.com/go/iqmagazine

or view the digital edition at this URL:

http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

CHAPTER 1

Product Overview

This chapter provides an overview of the Cisco 12006 and Cisco 12406 series routers. It contains physical descriptions of the router hardware and major components, and functional descriptions of the hardware-related features.

Introduction

The routers described in this guide are part of the Cisco 12006 and Cisco 12406 series routers and include:

- The original Cisco 12006 and Cisco 12406 series routers.
- The Cisco 12006 and Cisco 12406 enhanced series routers. The enhanced series of routers use higher capacity power supplies, a more powerful blower module, and have a new front door.

Note Most illustrations are shown without the new front door for clarity.

These two router models are differentiated by the switching capacity of the switch fabric installed in the router:

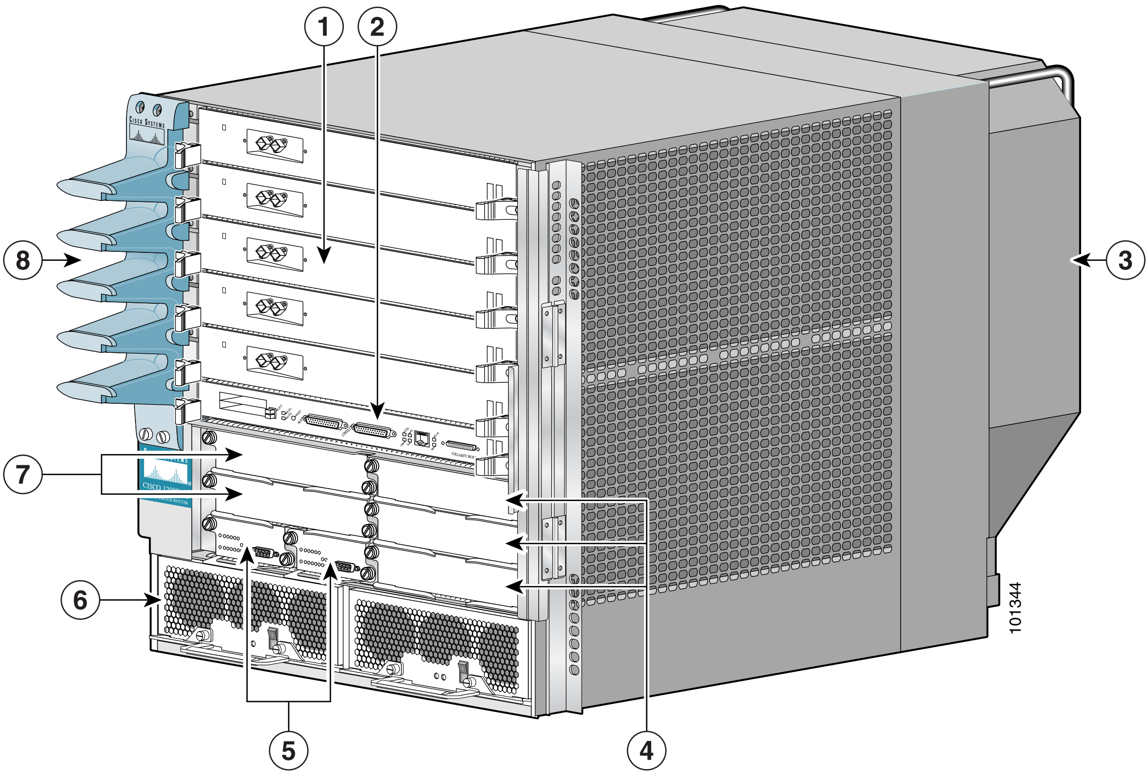
- Cisco 12006 Router—2.5-Gbps switch fabric
- Cisco 12406 Router—10-Gbps switch fabric

Other than their various capacities, these routers are almost identical. Differences between each router are described unless otherwise noted, all information in this publication applies to all routers.

Product Description

The Cisco 12006 and Cisco 12406 routers, shown in Figure 1-1, are members of the Cisco 12000 series router family. These routers are aimed at scaling the Internet and enterprise backbones to speeds of 155 Mbps (OC-3/STM-1), 622 Mbps (OC-12/STM-4), 2.4 Gbps (OC-48/STM-16), and 10 Gbps (OC-192/STM).

Figure 1-1 Cisco 12006 and Cisco 12406 router (Front View)



1	Line card slots (five)	**5**	Alarm card slots (two)
2	RP slot	**6**	Power module bays (two)
3	Blower module	**7**	CSC slots (two)
4	SFC slots (three)	**8**	Cable-management bracket

With a chassis height of 18.5 inches (46.9 cm), four Cisco 12006 and Cisco 12406 routers can be installed in a single standard 7-foot (2.15-m) equipment rack.

Cisco 12006 and Cisco 12406 routers support system software downloads for most Cisco IOS software upgrades, which enables you to remotely download, store, and boot from a new Cisco IOS image.

Cisco 12006 and Cisco 12406 routers have the following key features:

- Route Processor (RP)—Slot 5 (bottom slot) is the recommended slot for the first RP. When the router is equipped with a redundant RP, it can be installed in any of the five regular line card slots.
- Line Cards—Up to five OC-192 line cards, four if redundant RPs are installed. These slots support the online insertion and removal (OIR) feature so installed cards are hot-swappable: A failed card can be removed and replaced with the router powered on.
- Clock and Scheduler Cards (CSCs) and Switch Fabric Cards (SFCs)—Two dedicated hot-swappable slots for CSCs; three dedicated hot-swappable slots for SFCs.

Note The Cisco 12006 Router uses 2.5-Gbps switch fabric; the Cisco 12406 Router uses 10-Gbps switch fabric. You cannot mix 2.5-Gbps switch fabric cards and 10-Gbps switch fabric cards in a chassis. The router will not operate with a mix of switch fabric card types.

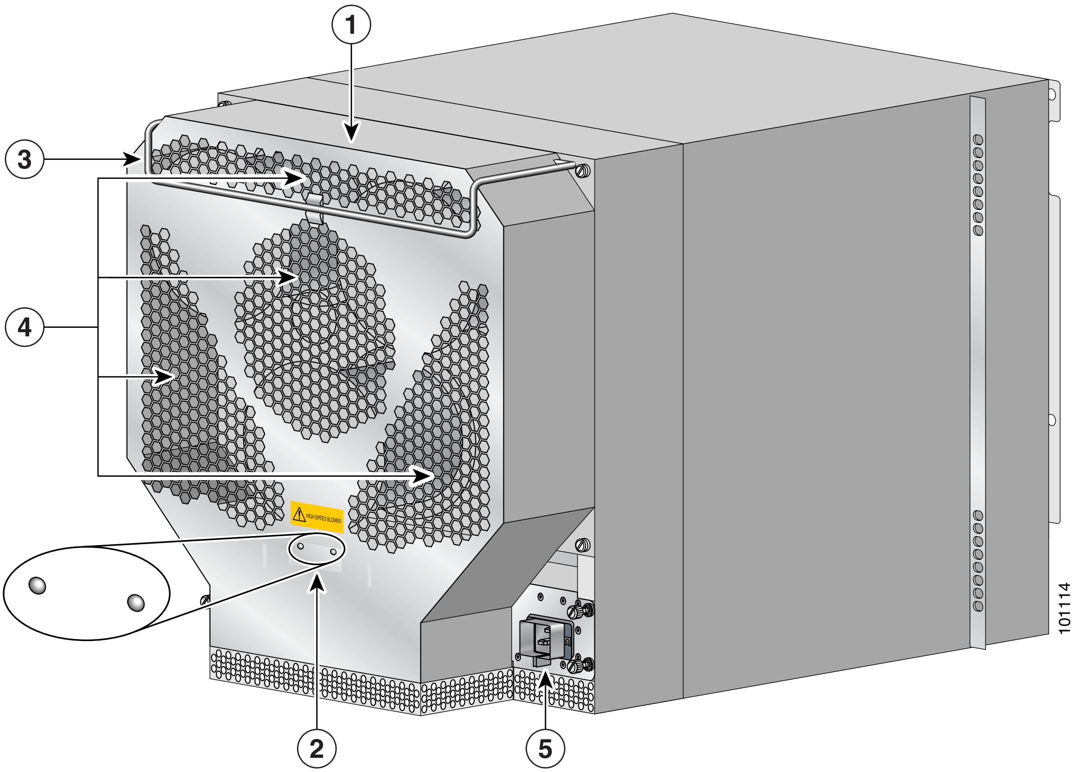
Note When operating your router with a single CSC, the second CSC slot must have a CSC blank filler (MAS-GSR6-CSCBLNK=) installed to ensure EMI compliance.

- Two dedicated alarm card slots (for 1+1 redundancy)
- Alarm and Illumination—Alarm and illumination for operating ranges in the card cage, clock and scheduler card, and switch fabric card bays.
- Two hot-swappable AC-input power supplies or DC-input power entry modules (PEMs).

Note When operating your router on a single AC-input power supply or DC-input PEM, the second power module bay must have a blank filler (MAS-GSR-PWRBLANK=) installed to ensure EMI compliance.

- All power modules and other field replaceable units (FRUs), except for the air blower module and the power distribution unit (PDU), can be removed from the front of the chassis.
- All source power connections are located at the rear of the chassis on the PDU. (See Figure 1-2.)
- Enhanced models have a new stylish front door that hides router cabling. The door can be installed to open from the right side or left side to give you total flexibility.
- Network Equipment Building Systems—Cisco 12006 and Cisco 12406 routers comply with the Network Equipment Building System (NEBS) Criteria Level 3 requirements defined in SR-3580 for flammability, structural, and electronics compliance.
- Electromagnetic Compatibility and Electrostatic Discharge Compliant—Cisco 12006 and Cisco 12406 routers comply with emissions, immunity, and electrostatic discharge (ESD) standards for both product and packaging.
- Bonding and Grounding—Bonding and grounding for safety, circuit protection, noise currents, reliability, and operations compliance.
- Environmental Monitoring—Cisco 12006 and Cisco 12406 router complies with environmental monitoring standards for operating temperature and humidity, as well as handling temperature and humidity (except for heat dissipation).
- Shock and Vibration—Cisco 12006 and Cisco 12406 routers have been shock- and vibration-tested for operating ranges, handling, and earthquake standards to NEBS (Zone 4 per GR-63-Core). These tests have been conducted in earthquake environment and criteria, office vibration and criteria, transportation vibration and criteria, and packaged equipment shock criteria.

Figure 1-2 Cisco 12006 and Cisco 12406 router (Rear View)



1	Blower module	**4**	Air exhaust vents
2	Blower module LEDs	**5**	PDU (behind Blower module; AC PDU shown)
3	Blower module handle	**–**	–

- Fiber Cable Management—Fiber cable management with support for high-density fiber Fast Ethernet (FE) ports.
- Current 1.275-inch pitch line cards will fit in the line card cage with the addition of a front panel adapter cover. The line card adapter cover is included with the 1.275-inch line card.

Physical and Functional Description

The main physical components of Cisco 12006 and Cisco 12406 routers and their functions are described in the following sections:

- Chassis, page 1-7
- Multigigabit Crossbar Switch Fabric, page 1-10
- Maintenance Bus, page 1-13
- Route Processors, page 1-15
- Line Cards, page 1-33
- Alarm Cards, page 1-35
- Power Subsystems, page 1-37
- Blower Module, page 1-47
- Air Filters, page 1-49
- Cable-Management System, page 1-50

Chassis

The Cisco 12006 and Cisco 12406 router chassis is an enclosure that consists of two integral card cages and two power module bays. (see Figure 1-1.)

RP and Line Card Slots

The RP and line card cage has six user-configurable slots that support one RP and up to five line cards. Network interfaces reside on the line cards that connect the switch fabric of the router to the external networks. For more information about the role of the RP, see the "Route Processors" section on page 1-15. For more information about the role of the line cards, see the "Line Cards" section on page 1-33.

Note Cisco 12006 and Cisco 12406 routers use line cards that are compatible with other Cisco 12000 series routers.

Switch Fabric Card Slots

The switch fabric circuitry resides in five fabric card slots: two for CSCs and three for SFCs. (See Figure 1-1.) For more information about the role of the switch fabric circuitry, see the "Multigigabit Crossbar Switch Fabric" section on page 1-10.

Alarm Card Slots

Cisco 12006 and Cisco 12406 routers are equipped with two alarm cards. These cards are positioned beside one another and occupy two card slots directly under the CSC slots. (See Figure 1-1.) For more information about the role of the alarm cards, see the "Alarm Cards" section on page 1-35.

Note The two alarm cards occupy slots under the two CSC slots in the CSC card cage, but are not part of the switch fabric.

Chassis Backplane

All of the card cages are tied together electrically through a passive system backplane in the back of the chassis. Nearly all of the wiring and circuitry in the chassis is contained within or connected to the chassis backplane. The chassis backplane distributes DC power to all of the cards in the chassis as well as the blower module, and provides the physical communication pathway between cards, both for network data and system communication across the internal system maintenance bus (MBus).

Power

Because a Cisco 12006 or Cisco 12406 Router can be configured with either an AC-input power system or a DC-input power system, the power module bays will accept either AC-input power supply modules or DC-input PEMs. For more information about the power subsystems, see the "Power Subsystems" section on page 1-37.

Caution To ensure that the chassis configuration complies with the required power budgets, use the on-line power calculator. Failure to properly verify the configuration may result in an unpredictable state if one of the power units fails. Contact your local sales representative for assistance.

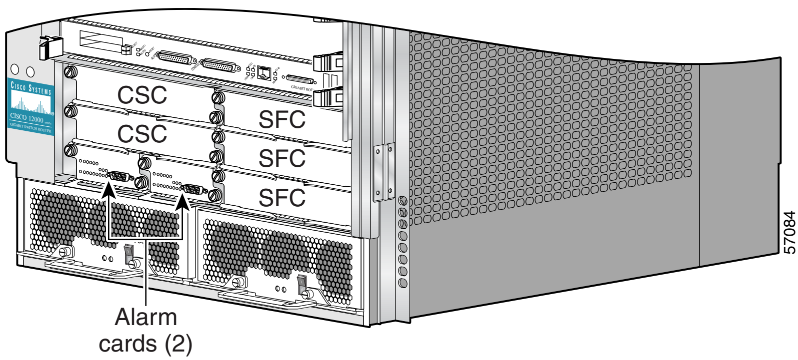
Cooling

Cisco 12006 and Cisco 12406 routers are equipped with a blower module to distribute air within the chassis. The blower module is a removable module located on the rear of the chassis. (See Figure 1-2.) For more information about the blower module, see the "Blower Module" section on page 1-47.

Multigigabit Crossbar Switch Fabric

Cisco 12006 and Cisco 12406 router switch fabric circuity provides synchronized gigabit-speed interconnections for the line cards and the RP. The switch fabric circuitry resides in five fabric card slots: two for CSCs; three for SFCs. (See Figure 1-3.)

Figure 1-3 Clock and Scheduler and Switch Fabric Card Bays



Switch Fabric Card Types

The CSCs are installed in the half-width slots labeled CSC 0 and CSC 1 on the lower left side of the chassis, located directly beneath the RP and line card cage and directly above the alarm card bays. The three SFCs are installed in the half-width slots labeled SFC 0, SFC 1, and SFC 2 on the lower right side of the chassis.

Note To operate, Cisco 12006 and Cisco 12406 routers must have at least one CSC card installed, in addition to SFC and alarm cards.

The CSC contains the following functionality:

- System clock—The system clock synchronizes data transfers between line cards or between the RP and a line card, through the switch fabric. In systems with redundant CSCs, the two system clocks are synchronized so that if one system clock fails, the other clock takes over. The system clock signal is sent to all line cards, the RP, and switch fabric cards.
- Scheduler—The scheduler handles requests from the line cards for access to the switch fabric. When the scheduler receives a request from a line card for switch fabric access, the scheduler determines when to allow the line card access to the switch fabric.
- Switch fabric—The switch fabric carries the user traffic between line cards or between the RP and the line cards. The switch fabric card contains only the switch fabric circuitry and receives scheduling information and system clock information from the CSC.

The SFC contains only the switch fabric circuitry, which carries user traffic between line cards or between the RP and the line cards. The SFC receives scheduling information and the system clock sent from the CSC.

Nonredundant and Redundant System Configurations

Cisco 12006 and Cisco 12406 routers are available in two system configurations:

1. Nonredundant configuration that includes one CSC and one power supply.

   When you order a Cisco 12006 or Cisco 12406 Router, the nonredundant configuration is shipped by default.

2. Redundant configuration that includes two CSCs and two power supplies.

For the redundant configuration, EMI compliance and cooling requirements are met by having two CSCs and two power supplies installed in the system.

For the nonredundant configuration, EMI compliance and cooling requirements are met only when blank fillers are installed in place of either (or both) the second (unused) CSC slot or the second (unused) power supply bay.

Note When operating your router with a single CSC, the second CSC slot must have a CSC blank filler (MAS-GSR6-CSCBLNK=) installed to ensure EMI compliance.

Switch Fabric Switching Capacity and Router Type

The Cisco 12006 Router is based on a 2.5-Gbps switch fabric, where each CSC or SFC provides a 2.5-Gbps full-duplex connection to each line card in the system. The 2.5-Gbps switch fabric consists of the 12006 Advanced Clock and Scheduler Card (product number 12006-CSC=) and the 12006 Advanced Switch Fabric Card (product number 12006-SFC=). The 2.5-Gbps switch fabric for the Cisco 12006 Router can be identified by the Cisco identification labels on the switch fabric cards (SFCs and CSCs): The CSC is labeled CSC-30/120 and the SFC is labeled SFC-30/120.

The Cisco 12406 Router is based on a 10-Gbps switch fabric, where each CSC or SFC provides a 10-Gbps full-duplex connection to each line card in the system. The 10-Gbps switch fabric consists of the Clock and Scheduler Card (product number GSR6-CSC=) and the Switch Fabric Card (product number GSR6-SFC=). The 10-Gbps switch fabric cards are labeled simply CSC and SFC.

Note You cannot mix 2.5-Gbps switch fabric cards and 10-Gbps switch fabric cards in a chassis. The router will not operate with a mix of switch fabric card types.

Switch Fabric Redundancy

Equipping the router with two CSCs provides data path, scheduler, and reference clock redundancy. The interfaces between the line cards and the switch fabric are monitored constantly. If the router detects a loss of synchronization (LOS), it automatically activates the data paths of the redundant CSC, and data flows across the redundant path. The switch to the redundant CSC occurs within 0.5 second, with little or no loss of data.

Maintenance Bus

The Cisco 12006 and Cisco 12406 router maintenance bus and MBus modules manage the maintenance functions of the system. The MBus is integrated into the backplane and consists of two separate buses, providing MBus redundancy.

Both MBus networks are linked to all the following items:

- Route processor and line cards
- CSCs, SFCs, and alarm cards
- Power modules
- Blower module

The MBus module located on each component communicates over the MBus and is powered by DC voltage directly from the alarm card. The MBus performs the functions of power-up/down control for each component, component (device) discovery, code download, diagnostics, and environmental monitoring and alarms.

Power-Up/Down Control

Each MBus module directly controls the DC-DC converters on the component on which it is mounted, based on commands the component receives from its on-board EPROM and from the RP. Each MBus module is tied directly to DC voltage from the alarm card.

When power is applied to the router, all MBus modules immediately power up. The MBus modules on the RP and CSC immediately turn on the DC-DC converter, powering up the respective card. The line card MBus module waits to power up the line card until it receives a command from the RP.

Device Discovery

The RP uses the MBus to detect the system configuration. The RP sends a message over the MBus requesting identity information from all installed devices. The responses provide component type, as well as slot numbers for the line cards, CSCs, SFCs, and alarm cards.

Code Download

A portion of the line card operating software can be downloaded from the RP to the line card over the MBus. Because the MBus is relatively slow compared to the switch fabric, only enough code is downloaded to the line card for it to access the switch fabric and complete the download process.

Diagnostics

The diagnostic software image is downloaded from the RP to the line card during the test sequence.

Environmental Monitoring and Alarms

The MBus module on each component monitors the environment of that component as follows:

- Line cards and the RP are monitored for temperature by two temperature sensors mounted on each card. The MBus module makes voltage adjustments through software for the +2.5 VDC, +3.3 VDC, and +5 VDC DC-DC converters.
- Clock and scheduler cards and switch fabric cards are monitored for temperature by two temperature sensors mounted on each card. The MBus module makes voltage adjustments through software for the +2.5 VDC and +3.3 VDC converters.
- The MBus module on the alarm card makes voltage adjustments for +5 VDC.
- Environmental monitoring includes voltage monitoring, temperature monitoring, and sensing for the blower module fans.

Route Processors

Each Cisco 12006 and Cisco 12406 router has one main system (or route) processor. The route processor (RP) processes the network routing protocols and distributes updates to the Cisco Express Forwarding (CEF) tables on the line cards. The RP also performs general maintenance functions, such as diagnostics, console support, and line card monitoring.

Route Processor Functions

The RP performs the following are primary functions:

- Downloading the Cisco IOS software to all of the installed line cards at power-up
- Providing a console (terminal) port for router configuration
- Providing an auxiliary port for other external equipment, such as modems
- Providing an IEEE 802.3, 10/100-megabit-per-second (Mbps) Ethernet port for Telnet functionality
- Running routing protocols
- Building and distributing routing tables to the line cards
- Providing general system maintenance functions for the router

The RP will function in any slot in the line card/RP card cage, but slot 5 is the recommended slot. If the router is equipped with an optional, redundant route processor, it can be installed in any of the remaining five slots.

The RP communicates with the line cards either through the switch fabric or through the MBus. The switch fabric connection is the main data path for routing table distribution as well as for packets that are sent between the line cards and the RP. The MBus connection allows the RP to download a system bootstrap image, collect or load diagnostic information, and perform general, internal system maintenance operations.

Route Processor Types

Two types of RPs are available for Cisco 12006 and Cisco 12406 routers, the Gigabit Route Processor (GRP), and the Performance Route Processor (PRP).

Each of these route processor types is reviewed in the following sections:

- Gigabit Route Processor, page 1-16
- Performance Route Processor, page 1-25

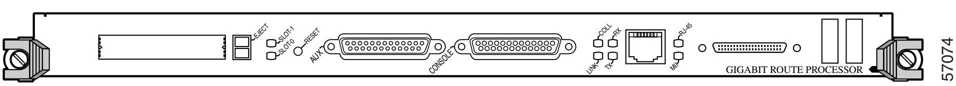
When not explicitly specified, this document uses the term route processor (RP) to indicate either the GRP or the PRP.

Note If you install a second RP for redundancy, the second RP must be of the same type as the primary RP.

Gigabit Route Processor

This section provides information about the GRP. The GRP front view is shown in Figure 1-4.

Figure 1-4 Gigabit Route Processor (Front View)



The GRP card has the following components:

- RISC processor—IDT R5000 Reduced Instruction Set Computing (RISC) processor used for the CPU. The CPU runs at an external bus clock speed of 100 MHz and an internal clock speed of 200 MHz.
- DRAM—Up to 512 megabytes (MB) of parity-protected, extended data output (EDO) dynamic random-access memory (DRAM) on two 60-nanosecond (ns), dual in-line memory modules (DIMMs). 128 MB of DRAM is the minimum shipping configuration for the GRP.

Note GRP route memory configurations of 512 MB are compatible with only Product Number GRP-B=. Cisco IOS Release 12.0(19)S or 12.0(19)ST or later, and ROMMON Release 11.2 (181) or later are also required.

- SRAM—512 kilobytes (KB) of static random-access memory (SRAM) for secondary CPU cache memory functions. SRAM is *not* user configurable or field upgradeable.
- NVRAM—512 KB of nonvolatile RAM (NVRAM). NVRAM is *not* user configurable or field upgradeable.
- Memory—Most of the additional memory components used by the system, including onboard Flash memory and up to two Personal Computer Memory Card International Association (PCMCIA)-based Flash memory cards and Advanced Technology Attachment (ATA) Flash disks.

  The GRP is shipped with 20 MB of Flash memory as the default configuration.
- Sensors—Air-temperature sensors for environmental monitoring.

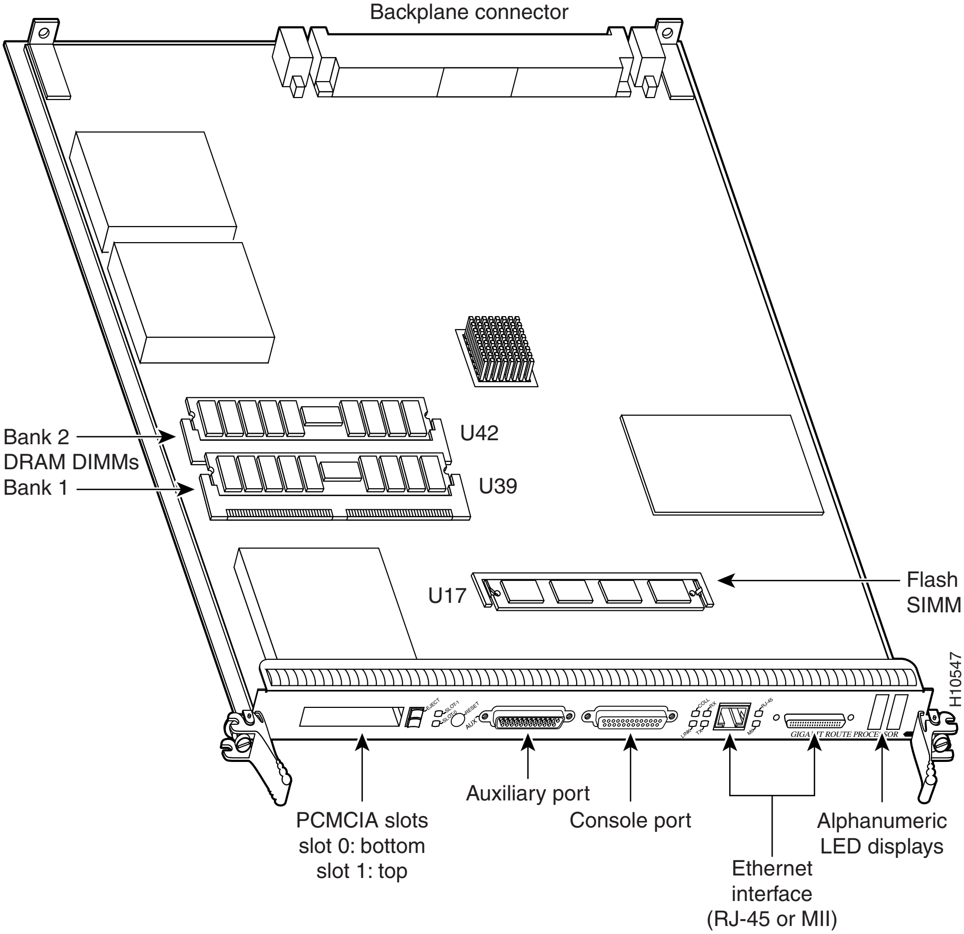
Note The GRP memory options and instructions for upgrading memory are described in the *Cisco 12000 Series Gigabit Switch Router Memory Replacement Instructions* (Document Number 78-4338-xx).

The Cisco IOS software images for operating the router reside in Flash memory on the GRP. The Flash memory can be either the single in-line memory module (SIMM) on the GRP or a PCMCIA Flash memory card that inserts into either PCMCIA slot 0 or slot 1 (labeled SLOT-0 and SLOT-1) on the front of the GRP. (See Figure 1-5.)

Note The GRP Flash memory SIMM contains the Cisco IOS software boot image, and a PCMCIA Flash memory card contains the Cisco IOS software image.

Storing the Cisco IOS images in Flash memory enables you to download and boot from upgraded Cisco IOS images remotely or from software images resident in GRP Flash memory. The Cisco IOS software runs from within GRP DRAM.

Figure 1-5 GRP Layout



GRP Memory Components

Table 1-1 lists the memory components on the GRP. Figure 1-5 shows the location of the DRAM and Flash SIMM on the GRP.

Table 1-1 GRP Memory Components

Type	Size	Quantity	Description	Location
DRAM	128[1] or 256 MB	1 or 2	64-MB or 128-MB DIMMs (based on DRAM required) for main Cisco IOS software functions	U39 (bank 1) U42 (bank 2)
SRAM	512 KB (fixed)[2]		Secondary CPU cache memory functions	—
NVRAM	512 KB (fixed)[2]		System configuration files, register settings, and logs	—
Flash Memory	8 MB SIMM[3]	1	Cisco IOS software images and other user-defined files	U17
	20 MB[4] Flash memory card	1 or 2	Cisco IOS software images, system configuration files, and other user-defined files on up to two Flash memory cars[5]	Flash memory card slot 0 and slot 1
Flash boot ROM	512 KB	1	Flash EPROM for the ROM monitor program boot image	

1. 128 MB of DRAM is the default DRAM configuration for the GRP.
2. This memory is neither user configurable nor field upgradeable.
3. SIMM socket is wired according to a Cisco design and does not accept industry-standard, 80-pin Flash SIMMs.
4. 20-MB Flash memory card is the default shipping configuration.
5. Type I or Type II PCMCIA cards can be used in either PCMCIA slot.

DRAM

The EDO DRAM on the GRP stores routing tables, protocols, and network accounting applications, and runs the Cisco IOS software. The standard (default) GRP DRAM configuration is 64 MB of EDO DRAM, which you can upgrade to 256 MB. Table 1-2 lists the DRAM configurations and upgrades.

Table 1-2 GRP DRAM Configurations

Total DRAM	Product Numbers	DRAM Sockets	Number of DIMMs
128 MB[1]	MEM-GRP/LC-64(=)	U39 (bank 1) and U42 (bank 2)	2 64-MB DIMMs
128 MB	MEM-GRP/LC-128(=)	U39 (bank 1)	1 128-MB DIMM
256 MB	MEM-GRP/LC-256(=)	U39 (bank 1) and U42 (bank 2)	2 128-MB DIMMs

1. 128 MB is the standard (default) DRAM configuration for the GRP.

Caution To prevent memory problems, DRAM DIMMs must be 3.3-volt (V), 60-nanosecond (ns) devices. Do not install other devices in the DIMM sockets. Cisco recommends that you use the Cisco-approved memory options listed in Table 1-2.

SRAM

SRAM provides secondary CPU cache memory. The standard GRP configuration is 512 KB. Its principal function is to act as a staging area for routing table updates and for information sent to and received from line cards. SRAM is *not* user configurable and *cannot* be upgraded in the field.

NVRAM

NVRAM provides 512 KB of memory for system configuration files, software register settings, and environmental monitoring logs. This information is backed up with built-in lithium batteries that retain the contents for a minimum of five years. NVRAM is *not* user configurable and *cannot* be upgraded in the field.

Flash Memory

Flash memory allows you to remotely load and store multiple Cisco IOS software and microcode images. You can download a new image over the network or from a local server and then add the new image to Flash memory or replace the existing files. You then can boot the routers either manually or automatically from any of the stored images.

Flash memory also functions as a Trivial File Transfer Protocol (TFTP) server to allow other servers to boot remotely from stored images or to copy them into their own Flash memory. The onboard Flash memory (called *bootflash)* contains the Cisco IOS boot image, and the Flash memory card contains the Cisco IOS software image. To order a spare Flash memory card, use Cisco product number MEM-GRP-FL20=, which is a 20-MB Type II PCMCIA Flash memory card.

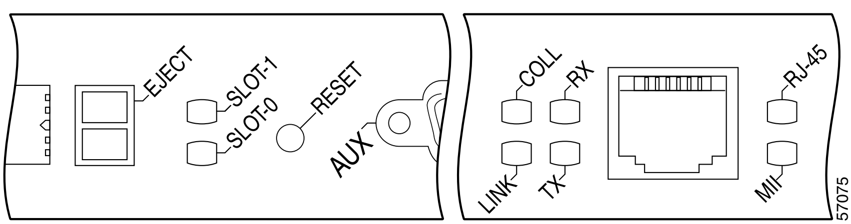
System Status LEDs

The GRP faceplate contains two types of system status LEDs: alphanumeric LED displays and device or port activity indicators.

The device or port activity indicators (see Figure 1-6) consist of the following functional groups:

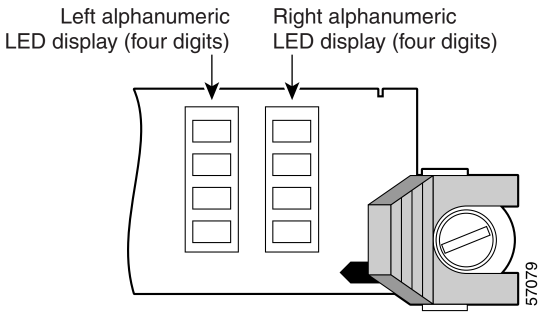
- Two Flash memory card activity LEDs (labeled SLOT-0 and SLOT-1)—one LED per Flash memory slot—Turns on when the slot is accessed.
- Four RJ-45 Ethernet port activity LEDs (labeled LINK, COLL, TX, and RX)—These LEDs are used only by the RJ-45 Ethernet connector and are disabled when the media-independent interface (MII) Ethernet port is in use. The LEDs indicate link activity (LINK), collision detection (COLL), data transmission (TX), and data reception (RX).
- Two Ethernet port selection LEDs (labeled MII and RJ-45)—When on, these LEDs identify which one of the two Ethernet connections you selected. When the RJ-45 port is selected, its LED is on and the MII LED is off. When the MII port is selected, its LED is on and the RJ-45 LED is off.

Figure 1-6 GRP LEDs (Partial Front Panel)



The alphanumeric LED displays (see Figure 1-7) are organized as two rows of four characters each. The content of the displays is controlled by the MBus module software. Both rows of the display are powered by the MBus module.

Figure 1-7 GRP Alphanumeric LED Displays (Partial Faceplate)



The alphanumeric LED displays router status messages:

- Router status messages that are displayed during the boot process
- Router status messages that are displayed after the boot process is complete

During the boot process, the alphanumeric LED message displays are controlled directly by the MBus module. After the boot process, they are controlled by the Cisco IOS software (through the MBus) and display messages designated by the Cisco IOS software.

The alphanumeric LED message displays also provide information about different levels of system operation, including the following:

- Status of the GRP
- Router error messages
- User-defined status and error messages

Note A complete, descriptive list of all system and error messages is located in the *Cisco IOS System Error Messages* publications.

Soft Reset Switch

The soft reset switch (see Figure 1-6) causes a nonmaskable interrupt (NMI) and places the GRP in ROM monitor mode. When the GRP enters ROM monitor mode, its behavior depends on the setting of the GRP software configuration register. (For more information on the software configuration register, see the "Configuring the Software Configuration Register" section on page 4-1.)

For example, when the boot field of the software configuration register is set to 0x0 and you press the NMI switch, the GRP remains at the ROM monitor prompt (rommon>) and waits for a user command to boot the system manually. If the boot field is set to 0x1, the system automatically boots the first Cisco IOS image found in the onboard Flash memory SIMM on the GRP.

Caution The soft reset (NMI) switch is *not* a mechanism for resetting the GRP and reloading the IOS image. It is intended for software development use. To prevent system problems or loss of data, use the soft reset switch only on the advice of Cisco service personnel.

Access to the soft reset switch is through a small opening in the GRP faceplate. To press the switch, you must insert a paper clip or similar small pointed object into the opening.

PCMCIA Slots

The GRP has two PCMCIA slots. Either slot can support a Flash memory card or an input/output (I/O) device, as long as the device requires only +5.2 VDC. The GRP supports only Type I and Type II devices. It does not support +3.3 VDC PCMCIA devices. Each PCMCIA slot has a button to eject the PCMCIA card from the slot.

Table 1-3 PCMCIA Devices (with GRP Oriented Horizontally)

PCMCIA Slot 0 (Bottom)	PCMCIA Slot 1 (Top)
Type I or II	Empty
Empty	Type I or II
Type I or II	Type I or II

Asynchronous Serial Ports

The console and auxiliary ports on the GRP are asynchronous serial ports used to connect external devices to monitor and manage the system. (See Figure 1-4.)

The console port is an Electronics Industries Association/Telecommunications Industry Association (EIA/TIA)-232 receptacle (female) that provides a data circuit-terminating equipment (DCE) interface for connecting a console terminal.

Note EIA/TIA-232 is also referred to as RS-232.

The auxiliary port is an EIA/TIA-232 plug (male) that provides a data terminal equipment (DTE) interface. The auxiliary port supports flow control and is often used to connect a modem, a channel service unit (CSU), or other optional equipment for Telnet management.

Note In order to maintain Class B EMI compliance, shielded cables must be used on the console and auxiliary ports of the GRP= and GRP-B=. An updated version of the GRP-B= board (Rev. F0) is available. This version does not require shielded cables for Class B compliance.

Ethernet Port

The GRP has one Ethernet port (see Figure 1-4), which uses one of the following two port connection types:

- RJ-45 receptacle—An 8-pin media-dependent interface (MDI) RJ-45 receptacle for either an IEEE 802.3 10BASE-T (10 Mbps) or an IEEE 802.3u 100BASE-TX (100 Mbps) connection.
- MII receptacle—A 40-pin media independent interface (MII) receptacle that provides additional flexibility in Ethernet connections.

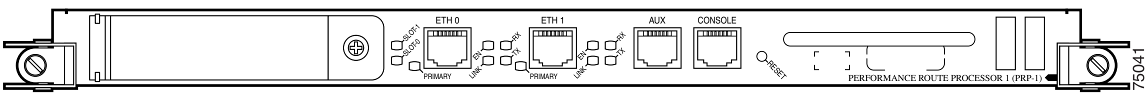
Note The RJ-45 and MII receptacles on the GRP represent two physical connection options for one Ethernet interface: you can use either the MDI RJ-45 connection or the MII connection, but not both simultaneously. The transmission speed of the Ethernet port is set through an auto-sensing scheme on the GRP.

The speed is determined by the network to which the Ethernet interface is connected, and is not user-configurable. Moreover, even at the auto-sensed data transmission rate of 100 Mbps, the Ethernet port provides maximum usable bandwidth of less than 100 Mbps. Expect a maximum usable bandwidth of approximately 20 Mbps when using either the MII or RJ-45 connection.

Performance Route Processor

This section provides information about the PRP. The PRP is supported in both the Cisco 12406 Router and the Cisco 12006 Router. Figure 1-8 shows the front panel view of the PRP. The PRP is shipped with 20 MB of Flash memory as the default configuration.

Figure 1-8 Performance Route Processor (Front View)



The PRP is available as Product Number PRP-1=, which includes one PRP with 512 MB of SDRAM and one 64-MB ATA Flash disk. A redundant PRP (Product Number PRP-1/R=) is also available.

The PRP contains the following components:

- PowerPC processor—Motorola PowerPC 7450 CPU, which runs at an external bus clock speed of 133 MHz and an internal clock speed of 667 MHz.
- SDRAM—Up to 2 GB of Cisco-approved SDRAM on two DIMMs. 512 MB of SDRAM is the default shipping configuration. SDRAM is field replaceable only when using Cisco-approved DIMMs.
- SRAM—2 MB of SRAM for secondary CPU cache memory functions. SRAM is *not* user configurable or field replaceable.
- NVRAM—2 MB of NVRAM. NVRAM is *not* user configurable or field replaceable.
- Memory—Additional memory components include onboard Flash memory and up to two Flash disks.
- Sensors—Air-temperature sensors for environmental monitoring.

The Cisco IOS software images are stored in Flash memory. Two types of Flash memory ship with the PRP:

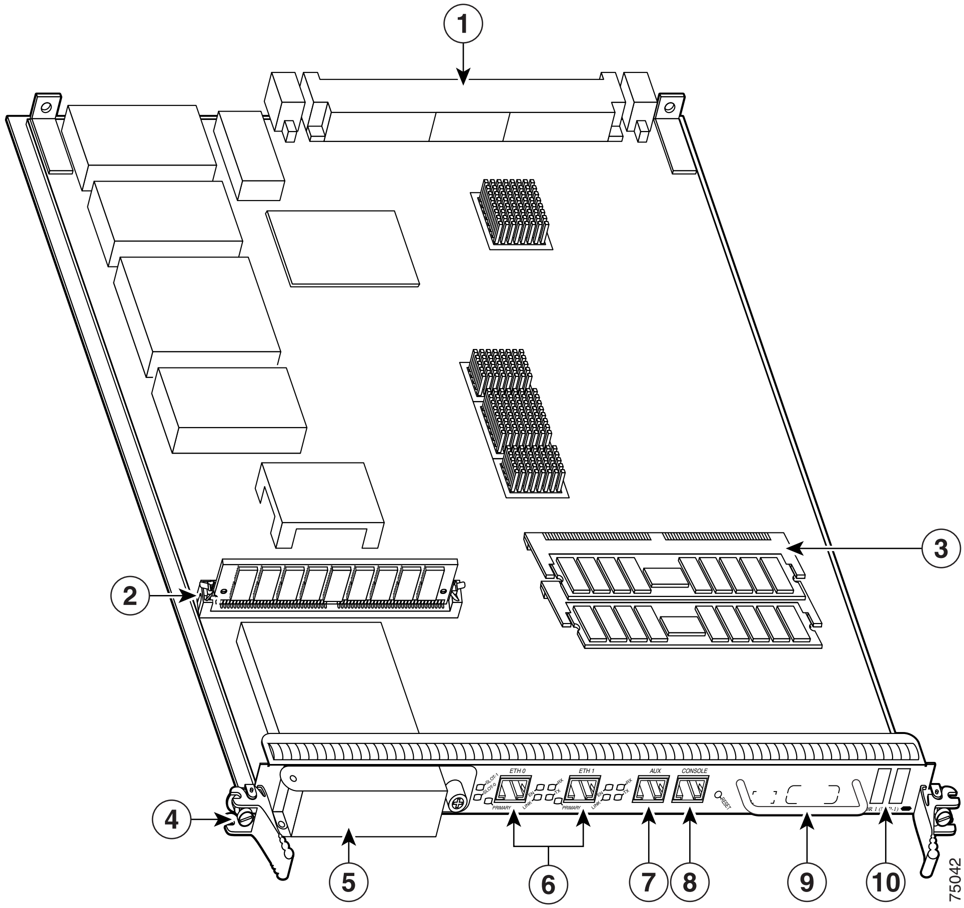
1. Onboard Flash memory—Ships as a single in-line memory module (SIMM). This Flash memory contains the Cisco IOS boot image (bootflash) and is not field replaceable.
2. Flash disk—The PRP ships with a Flash disk that can be installed in either Flash disk slot. (See Figure 1-9.) The Flash disk contains the Cisco IOS software image.

Storing the Cisco IOS images in Flash memory enables you to download and boot from upgraded Cisco IOS software images remotely, or from software images that reside in PRP Flash memory.

Cisco 12000 Series Routers support downloadable system software for most Cisco IOS software upgrades. This enables you to remotely download, store, and boot from a new Cisco IOS software image. The Cisco IOS software runs from within the SDRAM of the PRP.

Figure 1-9 shows the locations of the various hardware components on the PRP.

Figure 1-9 PRP (Horizontal Orientation)



1	Backplane connector	**6**	Ethernet ports
2	Flash SIMM (Socket number P3)	**7**	Auxiliary port
3	SDRAM DIMMs Bank 1 - Socket number U15 Bank 2 - Socket number U18	**8**	Console port
4	Ejector lever	**9**	Handle
5	Flash disk slots (covered)	**10**	Display LEDs

PRP Memory Components

PRP memory options and functions are listed in Table 1-4.

Table 1-4 PRP Memory Components

Type	Size	Quantity	Description	Location
SDRAM[1]	512 MB, 1 GB, or 2 GB	1 or 2	512-MB and 1-GB DIMMs (based on desired SDRAM configuration) for main Cisco IOS software functions	U15 (bank 1)[2] U18 (bank 2)
SRAM[3]	2 MB (fixed)	—	Secondary CPU cache memory functions	—
NVRAM[3]	2 MB (fixed)	1	System configuration files, register settings, and logs	—
Flash memory	64 MB SIMM[4]	1	Cisco IOS boot image (bootflash), crash information, and other user-defined files	P3
	64 MB, 128 MB, or 1 GB Flash disks[5]	1 or 2	Cisco IOS software images, system configuration files, and other user-defined files on up to two Flash disks	Flash disk slot 0 and slot 1
Flash boot ROM	512 KB	1	Flash EPROM for the ROM monitor program boot image	—

1. Default SDRAM configuration is 512 MB. Bank 1 (U15) must be populated first. You can use one or both banks to configure SDRAM combinations of 512 MB, 1 GB, or 2 GB. 1.5-GB configurations are not supported.
2. If both banks are populated, bank 1 and bank 2 must contain the same size DIMM.
3. This memory is neither user configurable nor field replaceable.
4. Flash memory SIMM is not user configurable or field replaceable.
5. ATA Flash disks and Type I and Type II linear Flash memory cards are supported. See the "Flash Memory" section on page 1-29 for Flash disk information.

Note If a single DIMM module is installed, it must be placed in bank 1 (U15).

SDRAM

SDRAM stores routing tables, protocols, and network accounting applications, and runs the Cisco IOS software. The default PRP configuration includes 512 MB of error checking and correction (ECC) SDRAM. DIMM upgrades of 512 MB and 1 GB are available. You cannot mix memory sizes. If two DIMMS are installed, they must be the same memory size.

Caution Cisco Systems strongly recommends that you use only Cisco-approved memory. To prevent memory problems, SDRAM DIMMs must be +3.3 VDC, PC133-compliant devices. Do not attempt to install other devices in the DIMM sockets.

SRAM

SRAM provides 2 MB of parity-protected, secondary CPU cache memory. It acts as a staging area for routing table updates and for information sent to and received from line cards. SRAM is *not* user configurable and *cannot* be upgraded in the field.

NVRAM

NVRAM provides 2 MB of memory for system configuration files, software configuration register settings, and environmental monitoring logs. This information is backed up with built-in lithium batteries that retain the contents for a minimum of 5 years. NVRAM is *not* user configurable and *cannot* be upgraded in the field.

Flash Memory

Flash memory allows you to remotely load and store multiple Cisco IOS software and microcode images. You can download a new image over the network or from a local server and then add the new image to Flash memory or replace the existing files. You then can boot the routers either manually or automatically from any of the stored images.

Flash memory also functions as a TFTP server to allow other servers to boot remotely from stored images or to copy them into their own Flash memory. The onboard Flash memory (called *bootflash)* contains the Cisco IOS boot image, and

the Flash disk contains the Cisco IOS software image. A 64-MB ATA Flash disk ships by default with the PRP. Table 1-5 lists the supported Flash disk sizes and their Cisco product numbers.

Table 1-5 Supported Flash Disk Sizes and Product Numbers

Flash Disk Size[1]	Product Number
64 MB[2]	MEM-12KRP-FD64=
128 MB	MEM-12KRP-FD128=
1 GB	MEM-12KRP-FD1G=

1. Standard Type 1 and Type 2 linear Flash memory cards also are supported, although they may not have the capacity to meet the requirements of your configuration.
2. 64-MB ATA Flash disk is the default shipping configuration.

System Status LEDs

The PRP faceplate is equipped with two types of system status LEDs: device or port activity indicators and alphanumeric LED displays.

The device or port activity indicators consist of the following functional groups:

- Two Flash disk activity LEDs (labeled SLOT-0 and SLOT-1)—one LED per Flash disk slot—Turns on when the slot is accessed.
- Four RJ-45 Ethernet port LEDs (labeled LINK, EN, TX, and RX)—Used in conjunction with each of the RJ-45 Ethernet connectors. Each connector includes a set of four LEDs that indicate link activity (LINK), port enabled (EN), data transmission (TX), and data reception (RX).
- Two Ethernet connection LEDs (labeled PRIMARY)—These two LEDs, when on, identify which of the two Ethernet connections is selected. Because both ports are supported on the PRP, the LED on port ETH0 is always on. The ETH1 LED goes on when it is selected.

The alphanumeric display LEDs are organized as two rows of four characters each and are located at one end of the card. (See Figure 1-7.) These LEDs display system status and error messages generated during and after the boot process. The boot process and the content displayed are controlled by the MBus module software on the PRP.

At the end of the boot process, the LEDs are controlled by the Cisco IOS software (via the MBus), and the content displayed is designated by the Cisco IOS software.

The display LEDs indicate the following information:

- Status of the PRP
- System error messages
- User-defined status and error messages

Note A complete, descriptive list of all system and error messages is located in the *Cisco IOS System Error Messages* publications.

Soft Reset Switch

The soft reset switch causes a nonmaskable interrupt (NMI) and places the PRP in ROM monitor mode. When the PRP enters ROM monitor mode, its behavior depends on the setting of the PRP software configuration register. (For more information on the software configuration register, see the "Configuring the Software Configuration Register" section on page 4-1. For example, when the boot field of the software configuration register is set to 0x0 and you press the NMI switch, the PRP remains at the ROM monitor prompt (`rommon>`) and waits for a user command to boot the system manually. If the boot field is set to 0x1, the system automatically boots the first IOS image found in the onboard Flash memory SIMM on the PRP.

Caution The soft reset (NMI) switch is *not* a mechanism for resetting the PRP and reloading the IOS image. It is intended for software development use. To prevent system problems or loss of data, use the soft reset switch only on the advice of Cisco service personnel.

Access to the soft reset switch is through a small opening in the PRP faceplate. To press the switch, you must insert a paper clip or similar small pointed object into the opening.

Flash Disk Slots

The PRP includes two Flash disk (PCMCIA) slots. Either slot can support an ATA Flash disk or a Type 1 or Type 2 linear Flash memory card. The PRP ships by default with one 64-MB ATA Flash disk.

Note The PRP only supports +5 VDC Flash disk devices. It does *not* support +3.3 VDC PCMCIA devices.

The PRP supports different combinations of Flash devices. You can use ATA Flash disks, Type 1 or Type 2 linear Flash memory cards, or a combination of the two. Each Flash disk slot has an ejector button for ejecting a card from the slot.

Note Type 1 and Type 2 linear Flash memory cards may not have the capacity to meet the requirements of your configuration.

Ethernet Ports

The PRP has two 10/100 Mbps Ethernet ports, each using an 8-pin RJ-45 receptacle for either IEEE 802.3 10BASE-T (10 Mbps) or IEEE 802.3u 100BASE-TX (100 Mbps) connections. (See Figure 1-8.)

Note The transmission speed of the Ethernet ports is auto-sensing by default and is user configurable.

Asynchronous Serial Ports

The PRP has two asynchronous serial ports, the console and auxiliary ports. (See Figure 1-8.) These ports allow you to connect external serial devices to monitor and manage the system. Both ports use RJ-45 receptacles.

The console port provides a data circuit-terminating equipment (DCE) interface for connecting a console terminal. The auxiliary port provides a data terminal equipment (DTE) interface and supports flow control. It is often used to connect a modem, a channel service unit (CSU), or other optional equipment for Telnet management.

Line Cards

Cisco 12006 and Cisco 12406 routers come pre-installed with the number and type of line cards that you ordered. Line cards and RPs can be installed in two basic combinations to support RP redundancy and a variety of physical network media:

- Nonredundant RP—One RP and up to five Cisco 12000 Series Router line cards.
- Redundant RPs—Two RPs and up to four Cisco 12000 Series Router line cards.

Line cards can be installed in any slot—zero (0) through five (5)—in the card cage. Slot number 5 is the recommended default RP slot. Single-mode and multimode line cards are shown in Figure 1-10.

Line cards provide the interfaces to the router's external physical media. External connections are made from the front of the chassis to the connectors on the line card face plates. The line cards communicate with the RP and exchange packet data with each other through the switch fabric cards in the switch fabric and alarm card cage.

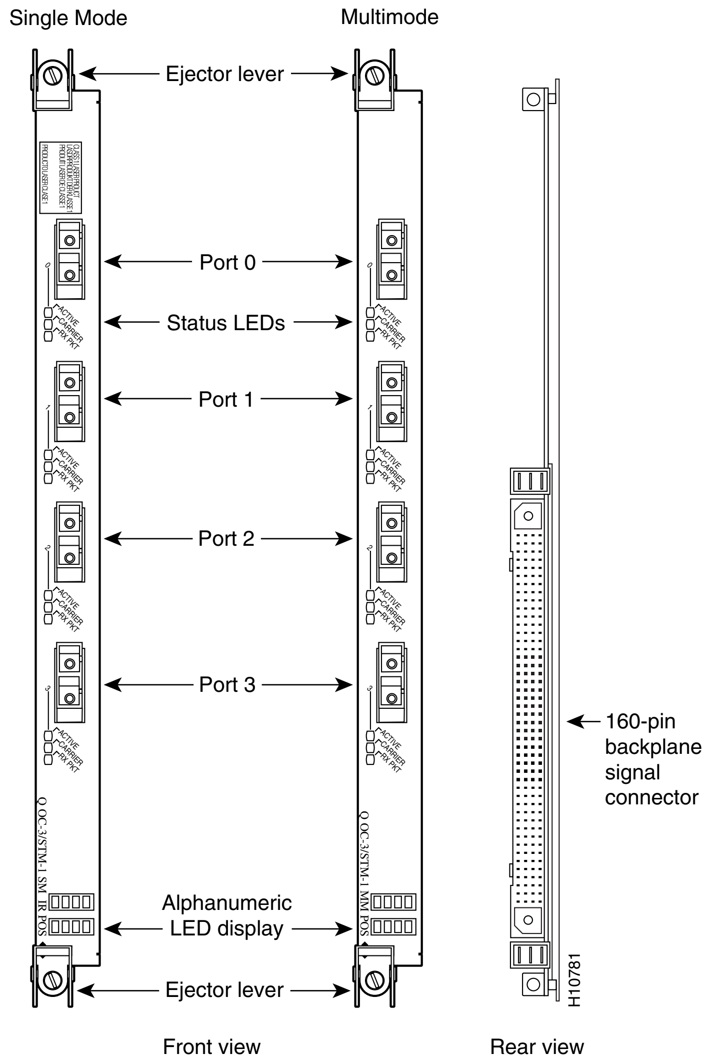
Caution Any unoccupied card slot in the line card and RP card cage must have a blank filler panel installed for electromagnetic compatibility (EMC) and to ensure proper air flow through the chassis. When the faceplate of a line card does not completely fill the card slot opening, a narrow card filler panel must be installed.

A cable-management bracket attaches to the faceplate of each line card to manage and organize the network interface cables connected to the individual ports on the line card.

Line cards installed in the router support online insertion and removal (OIR), which means you can remove and replace a line card while the router remains powered up.

Note For detailed instructions on removing, replacing, and configuring the line cards, see the configuration note shipped with each line card when ordered as an FRU.

Figure 1-10 Sample Line Cards



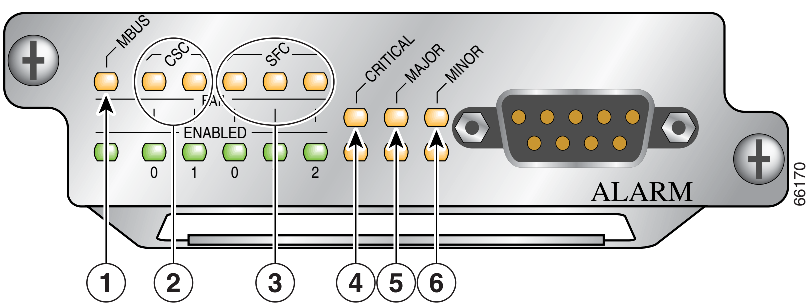
Alarm Cards

Cisco 12006 and Cisco 12406 routers have two alarm card slots. Each alarm card performs the following function or indicates the following condition:

- Alarm output
- CSC status
- SFC status
- Alarm card status
- Power source and power entry module status
- Alarm relay contacts

The entire alarm function has been implemented on redundant alarm cards with OIR maintenance (hot-swappable) functionality.

Figure 1-11 Alarm Card Features



1	MBus status LED	**5**	Major alarm LED
2	CSC status LEDs (two)	**6**	Minor alarm LED
3	SFC status LEDs (three)	**–**	Alarm relay contact connector
4	Critical alarm LED	**–**	–

Note Cisco 12006 and Cisco 12406 routers must be populated with two alarm cards, to meet EMI standards.

Alarm Output Function

The alarm output function consists of a group of relays, LEDs, and their associated drivers connected to an output port on the MBus module.

The alarm output function is controlled by the software on the RP. When a signal is received from the RP, the MBus module on the alarm card activates specific relays to signal an alarm condition. There are three alarm condition severity levels: critical, major, and minor. The critical, major, and minor LEDs are paired for redundancy to protect against a single failed LED.

Note Alarm cards for some Cisco 12000 series routers have both audible and visible alarm indicators. The alarm card for the Cisco 12006 and Cisco 12406 routers provides only visible alarm indicators as local alerts to unusual conditions in the router.

The IOS software running on the RP determines whether a given alarm condition is a critical, major, or minor alarm. Typing the show commands **sh gsr table** and **sh env all** will give you the table of limits and current readings for the LEDs.

Clock and Scheduler Card and Switch Fabric Card Status

The alarm card provides OK and FAIL indications for all clock and scheduler cards and switch fabric cards in the system. Redundant signals from the fabric cards are brought out to the LEDs on each alarm card. The alarm card does not control how these LEDs are used.

The MBus auxiliary power supply consists of a 50W DC-DC power supply and some current-sharing circuitry. Because the alarm card itself is powered by this supply, the on-board MBus module can report problems with the supply only when the redundant alarm card is in the chassis and providing MBus power.

Alarm Card Status

The ENABLED/FAIL pair of LEDs labeled MBUS indicate the status of the alarm card. The green ENABLED LED indicates that the MBus module on the alarm card is operating properly. The yellow FAIL LED indicates that the alarm card has detected an error in itself or with the MBus power supply.

Power Source Monitoring

The alarm card monitors the power modules and signals when there is a condition outside the normal range of operation. It discloses problems such as the following:

- Power source voltage is not being provided to a component
- A fault exists in the power source or power module
- Output voltage—Voltage monitor signal is outside the allowable range
- Output current—Current monitor signal is outside the allowable range

Alarm Relay Contact Connector

The 9-pin D-type alarm relay contact connector on the faceplate of the alarm card (see Figure 1-11) is used to connect external alarm indication equipment to the router so that alarm indicator signals in the router can be repeated elsewhere outside the router.

The pins on this connector are tied directly to the critical, major, and minor alarm relay contacts (normally open, normally closed, and common). Any event that causes one of the alarm LEDs on the alarm card faceplate to go on also activates the corresponding relay contact closure. The relay interface is rated at a maximum of 2A, 60V, or 50VA, whichever is greater.

Because alarm contact cables are entirely dependent on site-specific circumstances, alarm connector cables are not available from Cisco. For information about alarm connector wiring requirements and the pinout for the alarm connector interface, see the "Alarm Card Alarm Relay Connector Specifications" section on page A-6.

Power Subsystems

Cisco 12006 and Cisco 12406 routers can be powered by either an AC or DC power subsystem, as described in the following sections:

Note Cisco 12006 and Cisco 12406 routers can be either AC powered or DC powered; the router cannot accept two different types of power modules at the same time.

For detailed handling and replacement instructions for the Cisco 12006 and Cisco 12406 router power supplies or PEMs, see Chapter 6, "Maintaining the Router," or refer to the appropriate configuration note for the power supply or PEM that is shipped from the factory as an FRU.

Note Cisco 12006 and Cisco 12406 routers operating from an AC power source can be converted to operate from a DC power source, and vice versa. The conversion can be done in the field, but the system must be powered down. For more information about this conversion process, see the "Converting the Power System" section in the *Cisco 12006 and Cisco 12406 Router Power System Procedures Guide*.

AC Power Subsystem

The AC power subsystem consists of the following system components:

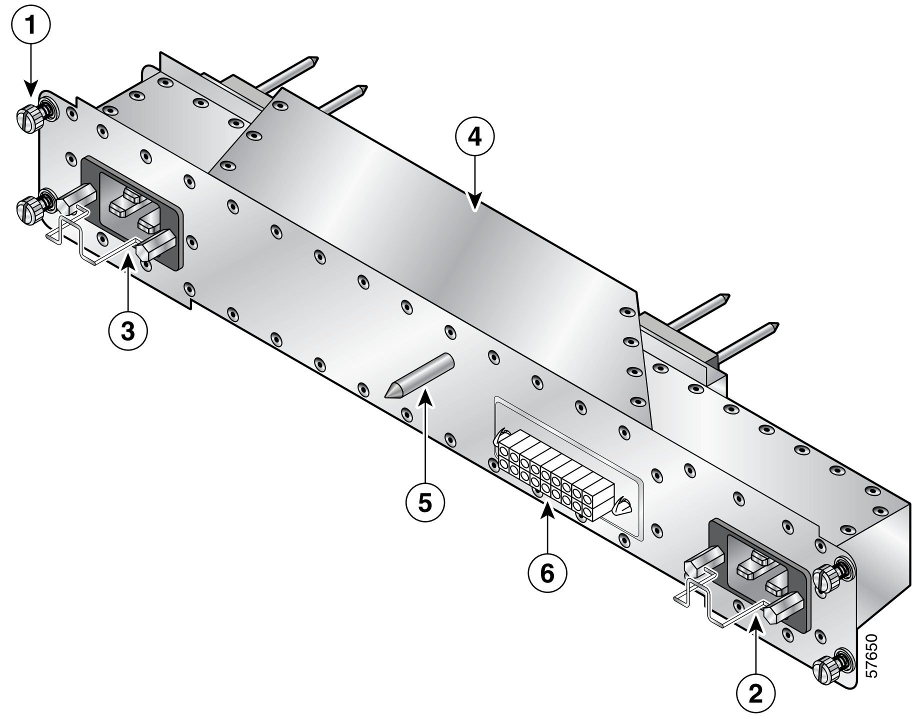
- AC PDU (one)
- AC-input power supplies (one for nonredundant operation; two for redundant operation)

Caution To ensure that the chassis configuration complies with the required power budgets, use the on-line power calculator. Failure to properly verify the configuration may result in an unpredictable state if one of the power units fails. Contact your local sales representative for assistance.

AC PDU

Facility AC power connects to AC-powered Cisco 12006 and Cisco 12406 routers though the AC PDU on the chassis rear panel. (See Figure 1-2 and Figure 1-12.)

Figure 1-12 AC Power Distribution Unit



1	Captive screw	**4**	AC power distribution unit
2	AC power cord receptacle A	**5**	Guide pin
3	AC power cord receptacle B	**6**	Blower module connector

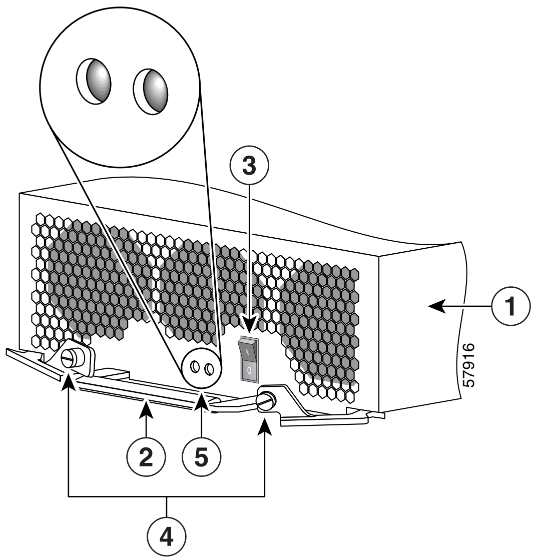
Depending on whether the router is configured for nonredundant or redundant power operation, the router ships with either one or two 14-foot (4.3-m) AC power cords to connect the PDU to the facility AC power source. AC power cords with different source AC power plugs are available. (See Figure 2-3 on page 2-15.)

Note For true redundancy, connect each power supply to a separate power circuit protected by its own circuit breaker.

AC-Input Power Supply

The AC-input power supply is a removable power module that installs in one of the bottom two bays on the front of the chassis (see Figure 1-1). These power modules support the OIR feature and are hot-swappable.

Figure 1-13 AC-Input Power Supply



1	AC-input power supply	**4**	Release levers captive screws
2	Handle	**5**	LEDs
3	Power standby switch	**–**	–

Note When operating your router on a single power module, the second power module bay must have a blank filler (MAS-GSR-PWRBLANK=) installed to ensure EMI compliance.

An AC-input power supply (shown in Figure 1-13) has the following features:

- A power factor corrector (PFC) allows the power supply to accept AC power source voltage from an AC power source operating from 100 to 240 VAC 20-amp service in North America, and a range of from 185 to 264 VAC 16-amp service in an international environment.
- Each AC-input power supply weighs 14 pounds (6.4 kg), and can deliver up to 1400 Watts (W) at –54.5 VDC.
- Each AC-input power supply requires a dedicated 20A service in North America (16A international).
- A power standby switch on the faceplate temporarily disables the DC output power circuitry in the AC-input power supply.

Note This switch does not interrupt the incoming AC power in the AC-input power supply. Portions of the power supply circuitry are still under AC power as long as AC power is connected to the router.

- A handle is provided for ease in removing and replacing the power supply.
- Captive screws on the power supply ejector levers secure it in the power supply bay.

- Two LEDs on the faceplate to provide status information. Table 1-6 summarizes the function of these indicators.

Table 1-6 AC-Input Power Supply LED indicators

LED Label	Function	State	Description
AC	Input power	On	AC power source is present and is within specified limits.
		Off	Power source is not within specified limits.
DC	Output Power	On	Power supply is operating normally in a power-on condition.
		Off	Power supply is operating in a fault condition and shutdown has occurred.

DC Power Subsystem

The DC power subsystem consists of the following system components:

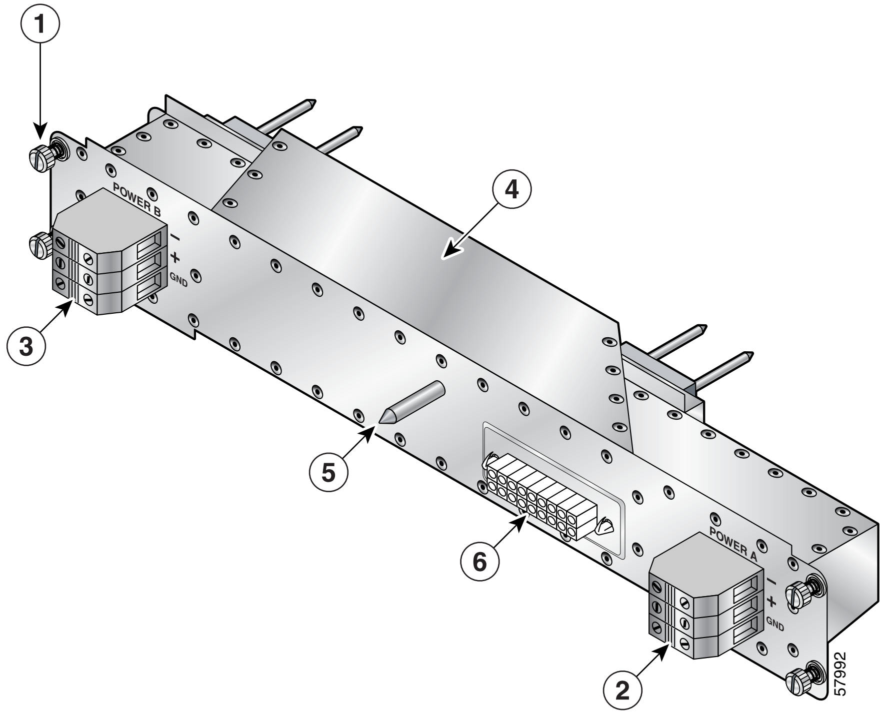
- DC PDU (one)
- DC-input PEMs (one for nonredundant operation; two for redundant operation)

Caution To ensure that the chassis configuration complies with the required power budgets, use the on-line power calculator. Failure to properly verify the configuration may result in an unpredictable state if one of the power units fails. Contact your local sales representative for assistance.

DC PDU

Facility DC power connects to DC-powered routers though the connector blocks on the DC PDU. (See Figure 1-2 and Figure 1-14.)

Figure 1-14 DC Power Distribution Unit

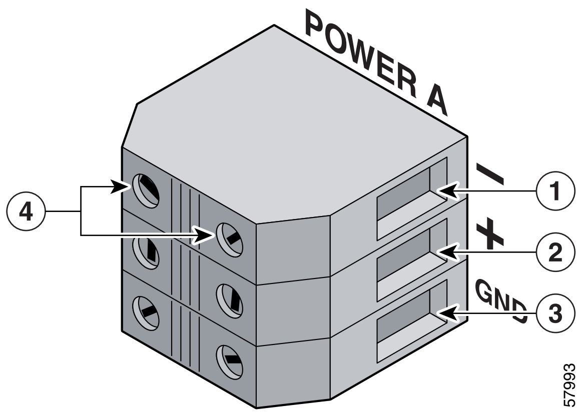


1	Captive screw	**4**	DC power distribution unit
2	DC power connector block A	**5**	Guide pin
3	DC power connector block B	**6**	Blower module connector

DC-input power is connected through the DC PDU on the chassis rear panel. The DC PDU is equipped with two DC power connector blocks. Each DC power connector block is equipped with three terminal ports. Leads from the DC source

power should be connected to the terminal block. A negative lead is connected to the top port, a positive lead to the middle port, and a ground lead to the bottom port. (See Figure 1-15.)

Figure 1-15 Cisco 12006 Router DC PDU Power Connector Block



1	Negative Terminal Port	**3**	Ground Terminal Port
2	Positive Terminal Port	**4**	Terminal Port Connector Screws

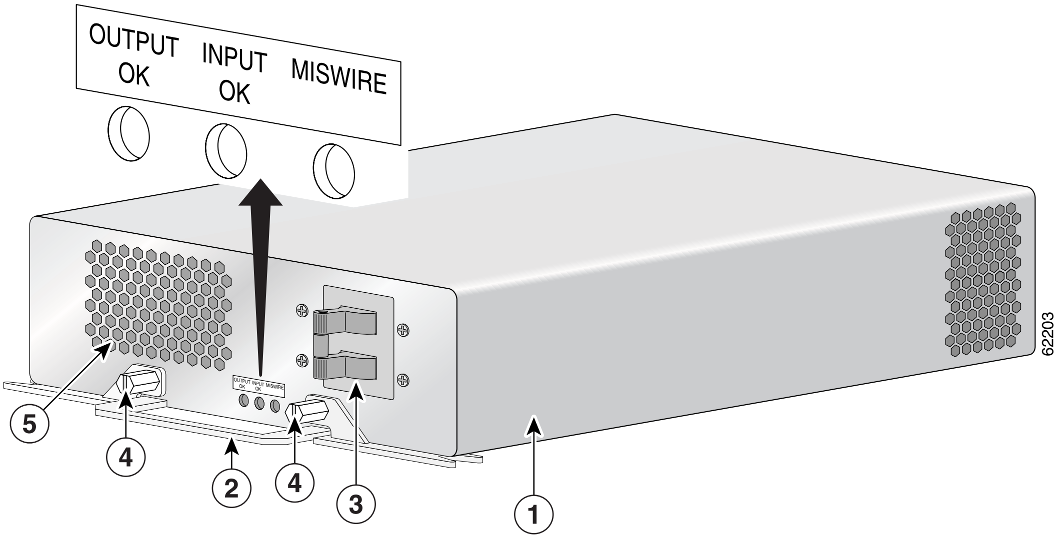
DC-Input Power Entry Module

The DC-input PEM is a removable power module that installs in one of the bottom two bays on the front of the chassis (see Figure 1-1). These power modules support the OIR feature and are hot-swappable.

Note When operating your router on a single power module, the second power module bay must have a blank filler (MAS-GSR-PWRBLANK=) installed to ensure EMI compliance.

Caution Cisco 12006 and Cisco 12406 routers are configured for either AC power or DC power. Do not mix AC-input power supplies and DC-input PEMs.

Figure 1-16 DC-Input Power Entry Module



1	DC-input PEM	**4**	Captive screws on release levers
2	Handle	**5**	Air inlet for cooling fan
3	Circuit breaker ON/OFF switch	**–**	–

A DC-input PEM (shown in Figure 1-16) has the following features:

- A circuit breaker switch on the faceplate turns the PEM on and off.
- A handle is provided for ease in removing and replacing the PEM.
- Captive screws on the PEM ejector levers secure it in the PEM bay.

- Three LEDs on the faceplate to provide status information. Table 1-7 summarizes the function of these indicators.

Table 1-7 DC-input PEM LED Indicators

LED Label	Color	Function
OUTPUT OK	Green	PEM is operating normally in a powered-on condition.
INPUT OK	Green	DC power is present at the PEM input and within the specified limits.
MISWIRE	Amber	Indicates input is wired backward at the PDU input.

- Each PEM weighs 10.5 pounds (4.76 kg), and can deliver up to 1400 W at –48 VDC.
- Only a DC power source that complies with the safety extra-low voltage (SELV) requirements in UL1950, CSA 950, EN 60950, and IEC950 can be connected to a PEM.
- Cisco 12006 and Cisco 12406 routers with a DC PDU and DC-input power entry modules (PEMs) require an external DC circuit breaker for each DC power source:
  - Original series Cisco 12006 and Cisco 12406 router input power shall not draw more than 45A max. @ 40.5VDC form each DC power source.
  - Enhanced series Cisco 12006 and Cisco 12406 router input power shall not draw more than 60A max. @ 40.5VDC from each DC power source.

  This circuit breaker should protect against short-circuit and overcurrent faults in accordance with United States National Electrical Code NFPA 70 (United States), Canadian Electrical Code, part I, CSA C22.1 (Canada), and IEC 364 (other countries).

Note Cisco Systems recommends that you install an uninterruptable power source (UPS) as a safeguard against power loss.

Power Distribution

The router chassis backplane distributes -48 VDC power throughout the router and to all cards in the card cages.

All cards have multiple DC-DC converters that convert the -48 VDC into +2.5 VDC, +3.3 VDC, +5 VDC, and other voltages as required by the line card. The DC-DC converters are turned on by the MBus modules under the control of the RP and MBus software.

Power for the blower module is supplied directly from the backplane through a connector in the PDU that passes DC voltage from the backplane to the blower module. An blower module controller card in the blower module converts –48 VDC into DC voltage that powers the blower module fans.

Caution To ensure that the chassis configuration complies with the required power budgets, use the on-line power calculator. Failure to properly verify the configuration may result in an unpredictable state if one of the power units fails. Contact your local sales representative for assistance.

Blower Module

Cisco 12006 and Cisco 12406 routers are equipped with a blower module to distribute air within the chassis. The blower module is located on the rear of the chassis. (See Figure 1-2.) The blower module draws room air into the chassis through two air filters on the side of the chassis, pulls the air through the chassis card cages, and expels it through exhaust vents on the back of the blower module. (See Figure 1-17.)

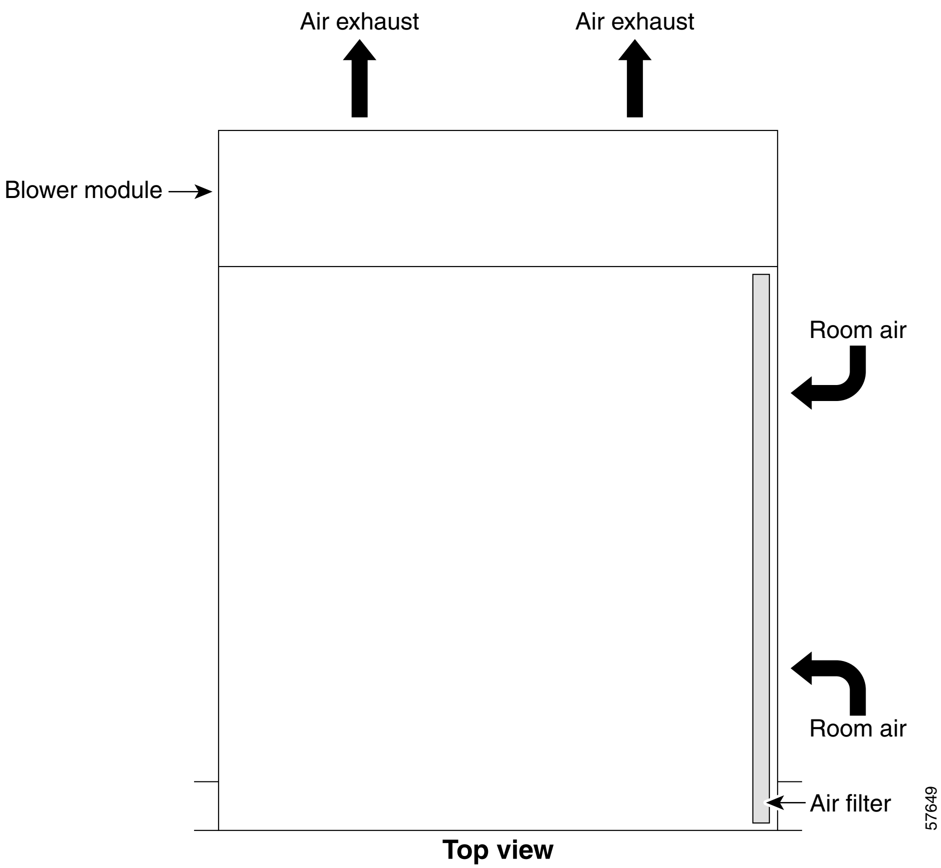
Caution Exhaust from other equipment vented directly into the router air inlet may cause overheating.

The front, back, and sides of the router must remain unobstructed to ensure adequate air flow and prevent overheating inside the chassis. Allow sufficient air flow by maintaining 6 inches (15.24 cm) of clearance at both the inlet and exhaust openings on the chassis.

If the air temperature inside the RP and line card cage rises, the system environmental monitor shuts down all internal power to prevent equipment damage from excessive heat.

If the system detects that one of three fans within a blower module has failed, it displays a warning message on the console screen. If multiple fans fail, the system shuts down to prevent equipment damage.

Figure 1-17 Internal Air Flow (Top View)



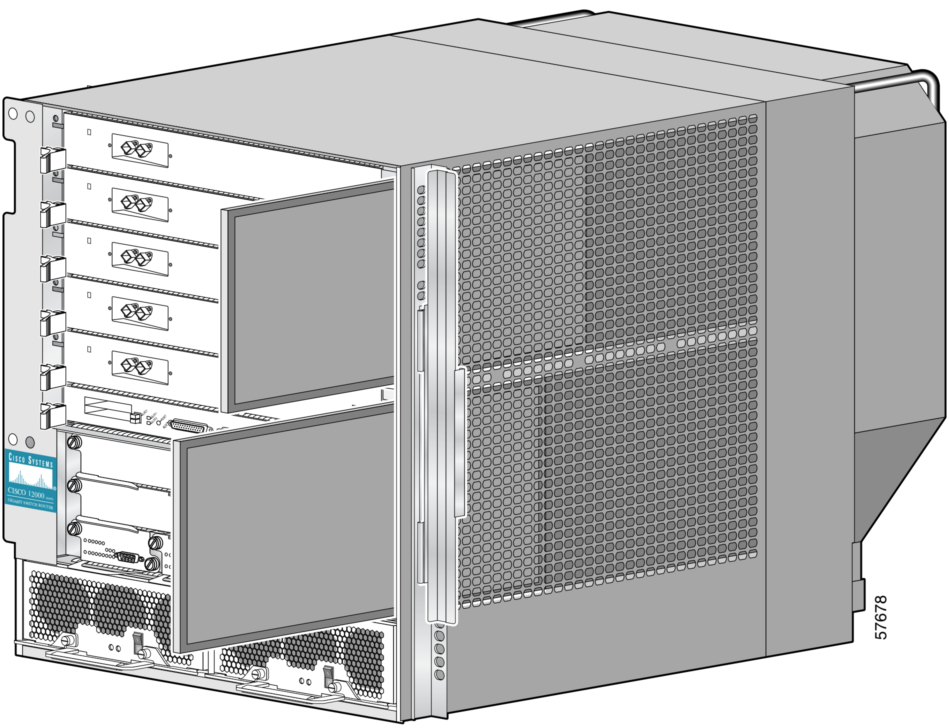
The two LEDs on the blower module provide a visual indication of blower module status. Both LEDs are visible on the blower module from the rear of the chassis.

- OK—Left LED; Green. When on, this LED indicates that the blower module is operating normally. This LED should come on as soon as the blower module is installed and receives power from the backplane connector.
- FAIL—Right LED; Red. The red LED should remain off during normal operation. If the red LED is on, the system has detected a fan failure or other fault in the blower module. Replace the existing blower module with a spare.

Air Filters

Cisco 12006 and Cisco 12406 routers are equipped with two user-serviceable air filters. (See Figure 1-18.)

Figure 1-18 Air Filter Locations



The air filters are located on the right of the front side of the chassis. The air filters are housed behind a door that is spring-loaded in the closed position.

Caution Air filters should be clean when the router is operating. Inspect and clean the air filters once a month, more often in dusty environments.

Do not run the router without the air filters installed. You should inspect and clean the air filters once a month, more often in dusty environments. Procedures for vacuuming and replacing the air filters are contained in the "Cleaning or Replacing the Air Filters" section on page 6-7.

Cable-Management System

The Cisco 12006 and Cisco 12406 router cable-management system organizes the interface cables entering and exiting the system, keeping them free of sharp bends and out of the way.

Caution Excessive bending in an interface cable can degrade performance.

The cable-management system (see Figure 1-19) consists of the following components:

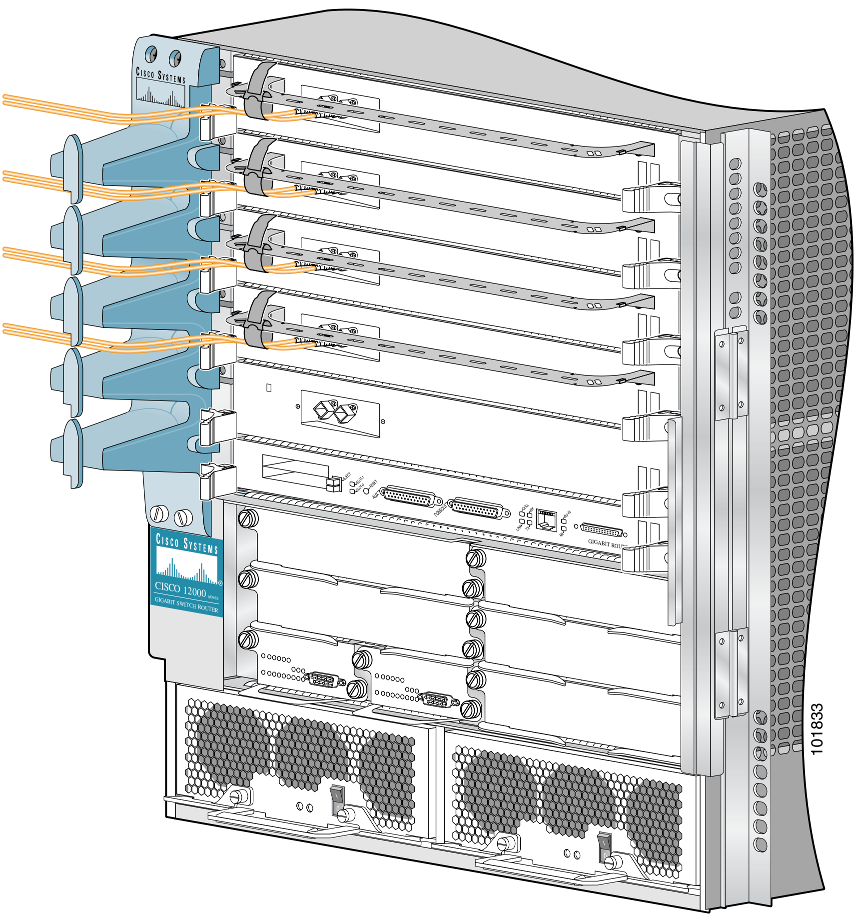
- One vertical cable-management bracket on the chassis
- One line card cable-management bracket on each line card

When you face the front of the router chassis, the chassis cable-management bracket is installed on the left side of the chassis, adjacent to the line card and RP card cage. The chassis cable-management bracket organizes the line card and RP cables to keep them from binding, and it eliminates interference when access to the front of the chassis is necessary for maintenance and reading the LEDs.

A line card cable-management bracket attaches to each line card with captive screws. Cable ties on the bracket hold the network interface cables in place, keep the cables organized relative to their assigned connectors, and manage the bend radius of each cable as it enters the connector on the line card.

On line cards with multiple ports, the line card cable-management bracket keeps the network interface cables organized when your remove and replace the line card. You can unplug the network interface cables from their connectors on the line cards and leave the cables bundled in the line card cable-management bracket while you remove the bracket from the line card. That way, when you replace the line card, the network interface cables are already aligned with the correct line card cable connectors.

Figure 1-19 Chassis Cable-Management System



Field-Replaceable Units

The field-replaceable units (FRUs) for Cisco 12006 and Cisco 12406 routers include the following units:

- Route processor
- Line cards
- CSCs
- SFCs
- Alarm cards
- PDU:
  - For AC powered systems, AC PDU
  - For DC-powered systems, DC PDU
- Power modules:
  - For AC-powered systems, AC-input power supplies
  - For DC-powered systems, DC-input PEMs
- AC power cords (for AC powered systems)
- Blower module
- Air filters
- Chassis cable-management bracket

Technical Specifications

For technical specifications and compliance information for Cisco 12006 and Cisco 12406 routers, see Appendix A, “Technical Specifications.”

CHAPTER 2

Preparing for Installation

This chapter provides specific information about preparing your site for the installation of Cisco 12006 and Cisco 12406 Routers. The following sections are included in this chapter:

Before installing a Cisco 12006 Router or Cisco 12406 Router, you should have the following information:

- Power and cabling requirements that must be in place at your installation site
- Equipment you will need to install the router
- Environmental conditions your installation site must meet to maintain normal operation

Note Do not unpack the router until you are ready to install it.

Tools and Equipment

Cisco 12006 and Cisco 12406 Routers can be installed with a minimum number of tools. The following tools are required:

- 1/4-inch and 3/16-inch flat-blade screwdrivers
- 9/16-inch wrench
- 10-mm wrench (either open-end or socket)
- 2-mm allen wrench
- ESD-preventive wrist strap
- Antistatic mat
- Tape measure
- Wire cutters
- Pliers

Safety and Compliance

The following guidelines help to ensure your safety and protect the equipment. This section does not include every potentially hazardous situation, so be alert.

- General Safety Guidelines, page 2-3
- Compliance and Safety Information, page 2-5
- Laser Safety, page 2-5
- Lifting Guidelines, page 2-5

General Safety Guidelines

- Never attempt to lift an object that might be too heavy for you to lift by yourself.

Caution *Do not* attempt to *lift* the chassis by the blower module handle. The blower module handle is intended for lifting the blower module only when it is disconnected from the chassis.

- Always disconnect the power source and unplug all power cables before lifting, moving, or working on the router.
- Keep the work area clear and dust free during and after installation.
- Keep tools and router components away from walkways and equipment rack aisles.
- Do not wear loose clothing, jewelry (including rings and chains), or other items that could get caught in the router.
- Fasten your tie or scarf and sleeves.
- Cisco equipment operates safely when it is used in accordance with its electrical ratings and product usage instructions.
- Do not work alone if potentially hazardous conditions exist.
- Always unplug the power cables when performing maintenance or working on the router, unless the replacement part is hot swappable and designed for online insertion and removal (OIR).
- The installation of the router should be in compliance with national and local electrical codes: in the United States, National Fire Protection Association (NFPA) 70, United States National Electrical Code; in Canada, Canadian Electrical Code, part I, CSA C22.1; in other countries, International Electrotechnical Commission (IEC) 364, part 1 through part 7.
- Before installing, configuring, or maintaining the router, review the safety warnings listed in the *Regulatory Compliance and Safety Information for the Cisco 12000 Series Router* (Document Number 78-4347-xx) that accompanied your router.

- Cisco 12006 and Cisco 12406 Routers with an AC power distribution unit (PDU) and AC-input power supplies are shipped with AC power cords equipped with three-wire electrical grounding-type plugs that will fit into only a grounding-type power outlet. This is a safety feature. The equipment grounding should be in accordance with local and national electrical codes.
- Cisco 12006 and Cisco 12406 Routers with a DC PDU and DC-input power entry modules (PEMs) require an external DC circuit breaker for each DC power source:
  - Original series Cisco 12006 and Cisco 12406 router input power shall not draw more than 45A max. @ 40.5VDC form each DC power source.
  - Enhanced series Cisco 12006 and Cisco 12406 router input power shall not draw more than 60A max. @ 40.5VDC from each DC power source.

  This circuit breaker should protect against short-circuit and overcurrent faults in accordance with United States National Electrical Code NFPA 70 (United States), Canadian Electrical Code, part I, CSA C22.1 (Canada), and IEC 364 (other countries).
- Only a DC power source that complies with the safety extra-low voltage (SELV) requirements in UL 1950, CSA-C22.2 No. 950, EN60950, ACA TS001, AS/NZS 3260, and IEC60950 should be connected to a Cisco 12006 or Cisco 12406 Router with DC PDU and DC-input PEMs.
- Cisco 12006 or Cisco 12406 Routers configured with DC-input PEMs should be installed in a restricted access area in accordance with Articles 110-16, 110-17, and 110-18 of the National Electric Code, ANSI/NFPA 70.
- Cisco 12006 or Cisco 12406 Routers configured with a DC PDU shall have a readily accessible disconnect device incorporated in the fixed wiring.

Compliance and Safety Information

The Cisco 12006 and Cisco 12406 routers are designed to meet the regulatory compliance and safety approval requirements. Refer to the *Regulatory Compliance and Safety Information for the Cisco 12000 Series Router* (Document Number 78-4347-xx) if you require additional compliance information (see "Cisco Technical Support and Documentation Website" section on page -xxfor site information).

Laser Safety

Single-mode Cisco 12000 Series Router line cards are equipped with lasers. The lasers emit invisible radiation. *Do not* stare into open line card ports. Observe the following warning to prevent eye injury:

Warning **Avoid exposure to laser radiation. Do not stare into an open aperture, because invisible laser radiation may be emitted from the aperture when a cable is not inserted in the port.**

Lifting Guidelines

A fully configured Cisco 12006 or Cisco 12406 Router weighs approximately 205 pounds (93 kg). Before you install the router, ensure that your site is properly prepared so that you will not have to move the router later to accommodate power source and/or network connections.

Caution To prevent damage, never attempt to lift or tilt the router chassis using the handles on the blower module or line cards. These handles do not support the weight of the chassis.

Whenever you lift any heavy or awkward equipment, follow these precautions to avoid injury to yourself or damage to the equipment:

- When using moving equipment, such as a safety hand truck, pallet jack, or forklift to move the equipment to another location, use only moving equipment that is capable of preventing the router from tipping.

- Have a second person help lift the equipment; avoid lifting the equipment alone.
- Ensure that your footing is solid; balance the weight of the object between your feet.
- Lift the equipment slowly; never move suddenly or twist your body as you lift.
- Keep your back straight and lift with your legs, not your back. If you must bend down to lift the equipment, bend at the knees, not at the waist, to reduce the strain on your lower back muscles.
- Always disconnect all external cables before lifting or moving the router.

Preventing Electrostatic Discharge Damage

Electrostatic discharge (ESD) damage to circuit boards can occur if proper grounding is not established. The boards can produce intermittent or complete failures if they are mishandled.

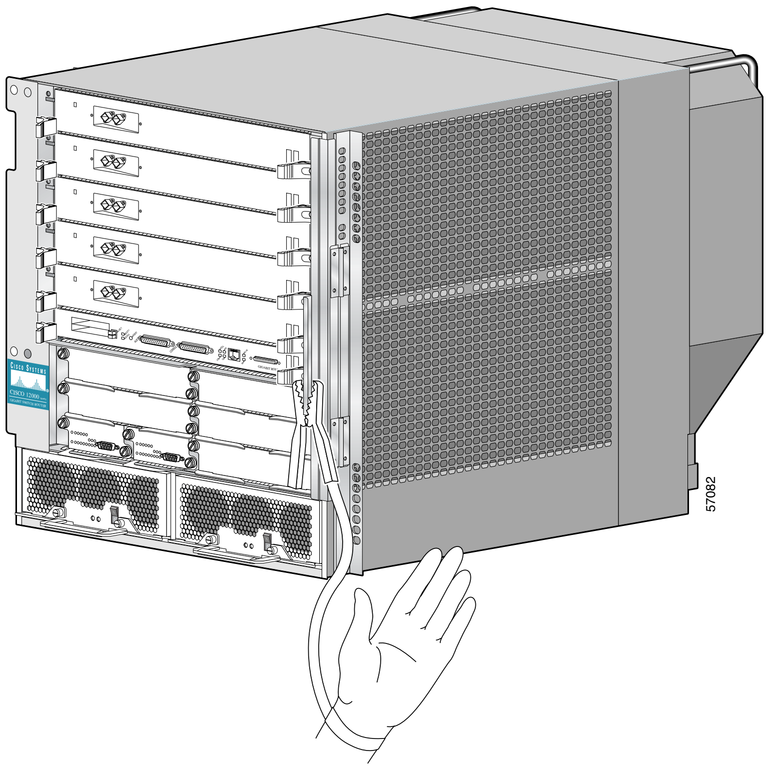
When handling circuit boards, observe the following guidelines to prevent ESD damage:

- Always use an ESD-preventive ankle or wrist strap and ensure that the strap makes adequate contact with your skin.
- The ankle or wrist strap protects equipment from ESD voltages on the body only; ESD voltages on clothing can still cause damage to electronic components.

Attaching an ESD-Preventive Strap

Attach an ESD antistatic strap to your body and to an open metal part of the chassis on the Cisco 12006 and Cisco 12406 Router (Figure 2-1).

Figure 2-1 Attaching an ESD-Preventive Strap to the Cisco 12006 and Cisco 12406 Router Chassis



Caution Periodically check the resistance value of the antistatic wrist strap. The resistance measurement should be between 1 and 10 megohms.

Safety with Electricity

The line cards, redundant clock and scheduler cards, switch fabric cards, alarm cards, blower module, and redundant power modules can be removed and replaced while the router is operating without presenting an electrical hazard or causing damage to the router.

Follow these basic guidelines when working with any electrical equipment:

- Before beginning any procedures requiring access to the interior of the router, locate the emergency power-off switch for the room in which you are working.
- Disconnect all external cables before installing or removing a router.
- Never assume that power has been disconnected from a circuit; always check.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Never install equipment that appears damaged.
- Carefully examine your work area for possible hazards such as moist floors, ungrounded power extension cables, and missing safety grounds.
- If an electrical accident does occur, proceed as follows:
  - Use caution; do not become a victim yourself. Disconnect power to the router.
  - If possible, send another person to get medical aid; otherwise, assess the condition of the victim and then call for help.
  - Determine if the person needs rescue breathing or external cardiac compressions, then take appropriate action.

In addition, observe the following guidelines when working with any equipment that is disconnected from a power source but still connected to telephone or network wiring:

- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines.

Site Requirement Guidelines

This section provides the site requirement guidelines that you must consider before installing Cisco 12006 and Cisco 12406 Routers:

- Environmental Guidelines, page 2-9
- Rack-Mounting Guidelines, page 2-10
- Power Connection Guidelines, page 2-14
- Site Wiring, page 2-20

Environmental Guidelines

This section offers guidelines for operating Cisco 12006 and Cisco 12406 Routers in various environments. The following environmental considerations are discussed:

- Airflow
- Temperature and humidity

Airflow

The air circulation system for Cisco 12006 and Cisco 12406 Routers consists of one blower module mounted at the rear of the chassis. The blower module maintains acceptable operating temperatures for the internal components by drawing cooling air in through replaceable air filters located on the right side of the chassis. Air circulates through the card cage and exhausts at the rear of the chassis.

Observe the following guidelines when selecting a site in which to install Cisco 12006 and Cisco 12406 Routers:

- Dust free—The site should be as dust free as possible. Dusty environments can clog the air filter or power supply intake vents, reducing the cooling air flow through the router. This can cause an overtemperature condition in the router.
- Air flow—Allow sufficient air flow by maintaining a minimum of 6 inches (15.24 cm) of clearance at both the inlet and exhaust openings on the chassis and the power modules. If the air flow is blocked or restricted, or if the inlet

air is too warm, an overtemperature condition can occur within the router. Under extreme conditions, the environmental monitoring system shuts down the power to protect the router components.

Temperature and Humidity

The operating environmental site requirements are listed in Appendix A, "Technical Specifications." The temperature and humidity ranges listed are those within which Cisco 12006 and Cisco 12406 Routers will continue to operate. You can maintain normal operation by anticipating and correcting environmental irregularities before they approach critical values.

The environmental monitoring functionality built into Cisco 12006 and Cisco 12406 Routers protects the system and components from potential damage from overvoltage and overtemperature conditions. To assure normal operation and avoid maintenance difficulty, plan and prepare your site before you install the router.

Rack-Mounting Guidelines

Before installing Cisco 12006 and Cisco 12406 Routers in a rack, consider the general rack-mounting guidelines in the following sections.

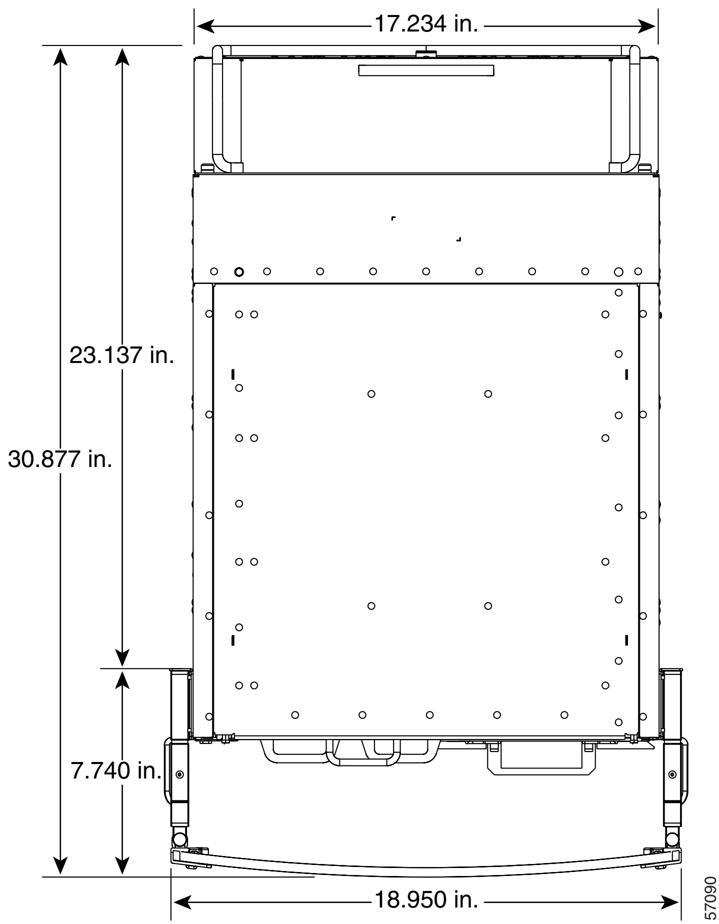
Types of Equipment Racks

Cisco 12006 and Cisco 12406 Routers can be mounted in most two-post, four-post, or telco-type 19-inch equipment racks that comply with the Electronics Industries Association (EIA) standard for equipment racks (EIA-310-D). The rack must have at least two posts with mounting flanges on which to mount the router chassis. The distance between the center lines of the mounting holes on the two mounting posts must be 18.31 inches ± 0.06 inch (46.50 cm ± 0.15 cm).

Equipment Dimensions and Site Layout

Figure 2-2 shows the footprint and outer dimensions of the chassis for Cisco 12006 and Cisco 12406 Routers.

Figure 2-2 Chassis Outer Dimensions and Footprint (shown with enhanced model front door)



To help maintain trouble-free operation, consider the following precautions when planning your rack installation:

- The site of the rack must include provisions for source AC or DC power, grounding, and network interface cables.
- For the actual installation, allow sufficient space to work around the rack. You will need at least 3 feet adjacent to the rack to move, align, and insert the chassis. You will need at least 2 feet in front of the chassis to insert power modules.
- Maintain at least 24 inches (61 cm) of clearance in front of and behind the chassis for maintenance after installation.
- To mount the router between two posts or rails, the usable aperture (the width between the *inner* edges of the two mounting flanges) must be at least 17.5 inches (44.5 cm).
- For the enhanced model of the Cisco 12006 and Cisco 12406 Routers, the mounting rails on a 4-post rack must be recessed no more than 1.5 inches for the front door to fully open and close and to provide adequate room for cable routing.
- The height of the Cisco 12006 and Cisco 12406 Router is 18.5 inches (46.9 cm). Most 7-foot (2.15-m) equipment racks will accommodate four Cisco 12006 and Cisco 12406 Routers. Allow sufficient space in the rack for the router.
- When fully populated with cards, Cisco 12006 and Cisco 12406 Routers can weigh as much as 205 pounds (93 kg). If you use a telco-style rack, the weight of the chassis is cantilevered off of the two rack posts. Ensure that the weight of the router does not make the frame unstable. Be sure that the frame is bolted to the floor and is secured to the building structure, either to wall or to overhead brackets.
- Do not route cables in such a way as to disrupt movement in front of or behind the rack. To avoid noise interference in network interface cables, do not route them directly across or along power cables. Use appropriate strain-relief methods to protect cables and equipment connections.
- Install and use the cable-management brackets included with the router to keep cables organized and out of the way of line cards, power modules, and blower modules. Consider the equipment and cabling that is already installed

in the rack. Ensure that cables from other equipment do not impair access to the card cages, requiring you to disconnect cables unnecessarily to perform equipment maintenance or upgrades.

Ventilation

The blower module is mounted at the rear of the chassis; air flow to the air filters and blower module should not be blocked.

Note Warm air is exhausted from the rear of the chassis. Maintain 6 inches (15.24 cm) of clearance at both the inlet and exhaust openings on the chassis to allow sufficient air flow.

- When placing multiple Cisco 12006 and Cisco 12406 Routers in the same rack, ensure that there is sufficient ventilation to accommodate the routers.
- Equipment located near the bottom of the rack can generate excessive heat that is drawn upward and into the intake ports of equipment above, possibly leading to overheating.
- The heated exhaust air from other equipment can enter the inlet air vents and cause overheating inside the router.
- A ventilation system that is too powerful in an enclosed rack can also prevent cooling by creating negative air pressure around the chassis and redirecting the air away from the air intake vent. If necessary, operate the router with the rack door open or in an open rack.
- The correct use of baffles inside an enclosed rack can assist in cooling the router.

Power Connection Guidelines

Cisco 12006 and Cisco 12406 Routers can be configured with either an AC-input power subsystem or a DC-input power subsystem. Site power requirements differ depending on which source power scheme is used. Follow these precautions and recommendations when planning power connections to the router:

- Check the power at your site before installation and periodically after installation to ensure that you are receiving clean power.
- If necessary, install a power conditioner.
- Install proper grounding to avoid damage from lightning and power surges.

Note When operating your router on a single power module, the second power module bay must have a blank filler (MAS-GSR-PWRBLANK=) installed to ensure EMI compliance.

Power Connection Guidelines for AC-Powered Routers

When the Cisco 12006 or Cisco 12406 Router operates with an AC PDU, observe these guidelines:

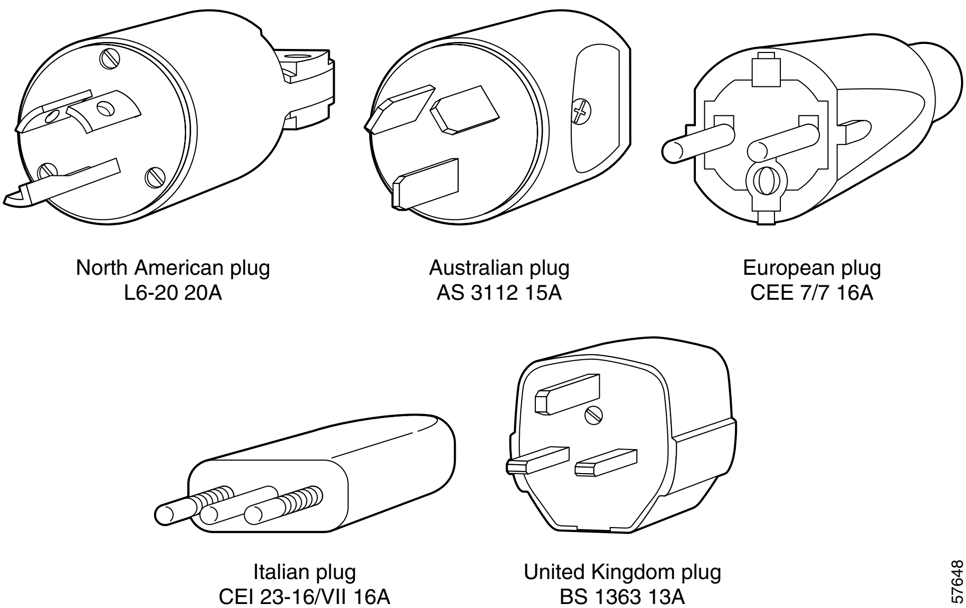
- A power factor corrector (PFC) allows the PDU to accept AC power source voltage from an AC power source operating between 100 and 240 VAC, 20A service in North America; and a range of from 185 to 264 VAC, 16A service, in an international environment.
- Use only the 14-foot (4.3-meter) AC power cords shipped with the system.
- Provide a dedicated power source with its own circuit breaker for each AC-input power supply installed in the router.
- Install an uninterruptable power source where possible.

Power plug types used in North America, Australia, and Europe are described in Table 2-1 and shown in Figure 2-3.

Table 2-1 AC-Input Power Cord International Options

Label	Description	Cisco Product Number
North America	20A, 250 VAC	CAB-GSR6-220V-US=
Australia, New Zealand	15A, 250 VAC	CAB-GSR6-AU=
Europe, Argentina, Brazil	16A, 250 VAC	CAB-GSR6-EU=
Italy	16A, 250 VAC	CAB-GSR6-IT=
United Kingdom	13A, 250 VAC (13A replaceable fuse)	CAB-GSR6-UK=

Figure 2-3 AC Power Plugs



Power Connection Guidelines for DC-Powered Routers

Be sure to observe the following guidelines for DC-powered Cisco 12006 and Cisco 12406 Routers:

- Cisco 12006 and Cisco 12406 Routers with a DC PDU and DC-input power entry modules (PEMs) require an external DC circuit breaker for each DC power source:
  - Original series Cisco 12006 and Cisco 12406 router input power shall not draw more than 45A max. @ 40.5VDC form each DC power source.
  - Enhanced series Cisco 12006 and Cisco 12406 router input power shall not draw more than 60A max. @ 40.5VDC from each DC power source.

  This circuit breaker should protect against short-circuit and overcurrent faults in accordance with United States National Electrical Code NFPA 70 (United States), Canadian Electrical Code, part I, CSA C22.1 (Canada), and IEC 364 (other countries).
- Provide a dedicated power source for each power entry module installed in the router.
- Install an uninterruptable power source where possible.

Grounding Connections

Before you connect power or turn on your Cisco 12006 or Cisco 12406 Router, you must provide an adequate system ground for the router. The equipment grounding should be in accordance with local and national electrical codes.

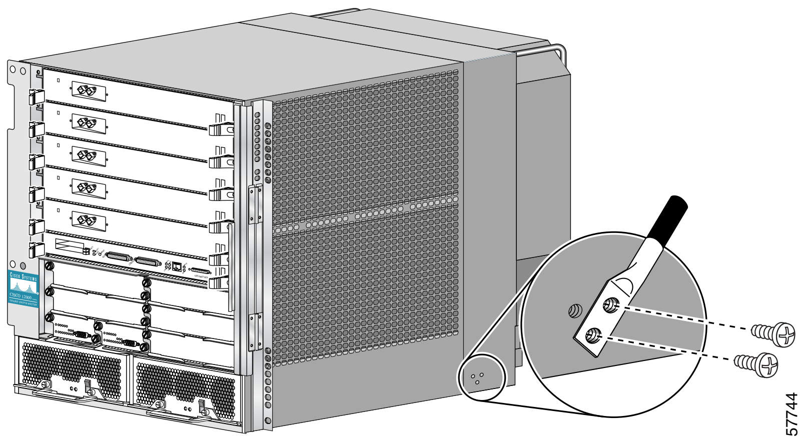
For installations other than in a network equipment building system (NEBS) environment, you may chose to rely on the safety earth ground connection supplied via the International Electrotechnical Commission (IEC) 320 inlets for AC-powered units and the main terminal block ground connection for DC-powered units.

- On Cisco 12006 and Cisco 12406 Routers configured for AC-input operation, the AC PDU is equipped with two three-wire electrical grounding-type connectors that accept three-wire, grounding-type AC power cords such as the power cords shipped with the router. This is a safety feature.

- On Cisco 12006 and Cisco 12406 Routers configured for DC-input operation, the DC PDU is equipped with two DC power connector blocks, each with wire-connection terminals for connecting the negative lead (top terminal), the positive lead (middle terminal), and the ground lead (bottom terminal). This is a safety feature.

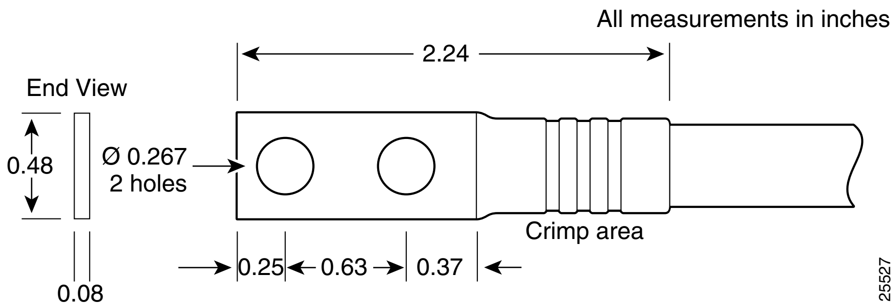
If the router is installed in a NEBS environment, we strongly recommend that you connect the central office ground system or interior equipment grounding system to the supplemental bonding and grounding point on the router chassis. This grounding point consists of three threaded inserts is located on the side of the chassis near the back of the chassis. (See Figure 2-4.) It is also referred to as the NEBS bonding and grounding receptacle, and is intended to satisfy the Telcordia NEBS requirements for supplemental bonding and grounding connections.

Figure 2-4 Supplemental Bonding and Grounding Port for NEBS Compliance



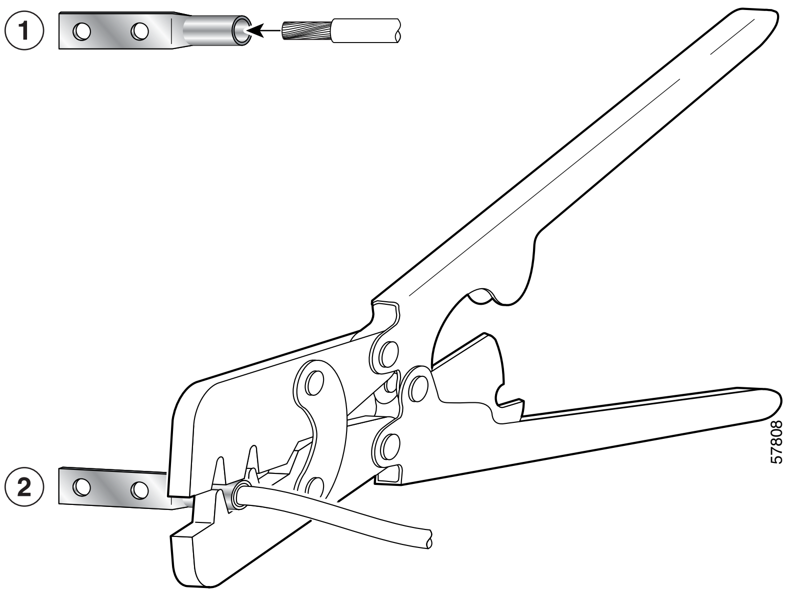
Use a cable lug with two holes at 0.63" (16 mm) centers to connect to the chassis with two 6.3 mm (M6) screws as shown in Figure 2-5. The lug can be ordered from Cisco (Part Number 32-0607-01).

Figure 2-5 Cable Lug



The dual-hole lug is crimped onto a grounding wire of a wire size and length determined by your router location and facility environment. The crimping tool shown in Figure 2-6 is a standard crimping tool obtainable from any normal hardware source.

Figure 2-6 Crimping the Lug



1	Place ground wire in the lug	**2**	Crimp the lug

Note The three threaded inserts that make up the grounding receptacle are set in a triangle so that you can choose any two of the three holes to attach the lug and grounding cable.

Site Wiring

This section presents site wiring guidelines for setting up the plant wiring and cabling at your site. When planning the location of the new system, consider the following:

- Electromagnetic interference (EMI)
- Distance limitations for signaling and unshielded conductors

Electromagnetic Interference

EMI can occur between the signals on the wires and external or ambient EMI fields when the wires are run for any significant distance. Bad wiring practice can result in radio interference emanating from the plant wiring.

Warning **Strong EMI, especially when it is caused by lightning or radio transmitters, can destroy the signal drivers and receivers in the Cisco 12006 and Cisco 12406 Router, can create an electrical hazard by conducting power surges through lines, and can damage the equipment.**

To predict and remedy strong EMI, you may need to consult experts in radio-frequency interference (RFI).

If you use twisted-pair cable in your plant wiring with a good distribution of grounding conductors, the plant wiring is unlikely to emit radio interference. If you exceed the recommended distances, use a high-quality twisted-pair cable with one ground conductor for each data signal when applicable.

Distance Limitations

If wires exceed recommended distances, or if wires pass between buildings, give special consideration to the effect of a lightning strike in your vicinity. The electromagnetic pulse (EMP) caused by lightning or other high-energy phenomena can easily couple enough energy into unshielded conductors to destroy electronic devices. If you have had problems of this sort in the past, you may want to consult experts in electrical surge suppression and shielding.

Most data centers cannot resolve the infrequent but potentially catastrophic problems just described without pulse meters and other special equipment. These problems can cost a great deal of time to identify and resolve, so take precautions by providing a properly grounded and shielded environment, with special attention to issues of electrical surge suppression.

Unpacking and Repacking the Router

The shipping package for Cisco 12000 series routers is engineered to reduce the potential of product damage associated with routine material handling experienced during shipment. To minimize potential damage to the product, transport these products in their Cisco-specified packaging. Failure to do so may result in damage to the router or degradation of its performance. Also, do not remove the Internet router from its shipping container until you are ready to install it. The router should always be transported or stored in an upright position. Keep the router in the shipping container until you have determined where you will install it.

Refer to the unpacking instructions (*Cisco 12006 and 12406 Router Unpacking and Repacking Instructions* document number 78-16104-xx) that came with the router to unpack it from the shipping pallet and verify the contents. This document also includes instructions to repack the router if you need to transport it.

If you do not receive everything you ordered, contact a customer service representative for assistance. See the section titled, Obtaining Technical Assistance, page -xx.

Site Preparation Checklist

Cisco 12006 and Cisco 12406 Routers come with a site log. Keep this in a common place near the router where anyone who performs tasks can have access to it. Site log entries might include the following:

- Installation progress—Make entries in the site log to record installation. Note any difficulties encountered and their remedies during the installation process.
- Upgrades and removal/replacement procedures—Use the site log as a record of system maintenance and expansion history, for example:
  - FRU installed, removed, or replaced
  - Configuration changes
  - Software upgrades
  - Corrective or preventive maintenance procedures performed
  - Intermittent problems
  - Your comments

Table 2-2 shows a sample site log. You can make copies of the sample or design your own site log.

Table 2-2 Sample Site Log

Date	Description of Action Performed or Symptom Observed	Initials

CHAPTER 3

Installing the Router

This chapter describes how to do the initial installation and setup of Cisco 12006 and Cisco 12406 Routers. It includes the following sections:

Installing a Router

This section explains the procedures for installing Cisco 12006 and Cisco 12406 Routers and contains the following sections:

Before installing Cisco 12006 and Cisco 12406 Routers, see Chapter 2, "Preparing for Installation," for information on environmental considerations and requirements.

Ensure the following before you install the router:

- The exhaust vents on the blower module mounted at the rear of the chassis are not blocked.
- The air filter is mounted on the right side as you face the router; air flow to the blower module is not blocked.
- There is 24 inches (61 cm) of clearance at the rear of the chassis so you can read the blower module LEDs and perform maintenance on the module.
- There is 24 inches (61 cm) of clearance in front of the router chassis to enable working with line cards and power supplies, and attaching Network Interface Cable (NICs) or other components.
- Location is temperature controlled, air conditioned, and dust free.
- Power cables and power supplies have been checked for compatibility with your power service.
- Labels on the equipment have been checked to ensure that the power service at your site is suitable for the router.
- AC power source receptacles are easy to reach.

Warning **Do not mix power module input types in the router. All power modules installed in a router must be either AC-input power supplies or DC-input PEMs.**

Installing the Rack-Mount Brackets (Optional)

The router accessory kit includes a pair of rack-mount brackets that can be used as a temporary aid to bear the weight of the router while it is being positioned in the equipment rack and secured. The use of these mounting brackets is optional; you can install the router in the rack without using these brackets. These brackets can be left in place following router installation.

Tools and Equipment Required

You need the following items to install the optional rack-mount brackets:

- Number 2 Phillips screwdriver
- Tape measure (optional)
- Level (optional)

Installing the Optional Rack-Mount Brackets

To install the rack-mount brackets, see Figure 3-1 and follow these steps:

Step 1 Measure and mark the hole at the same height on both the left and right rack rails.

Step 2 Mount the right mounting bracket:

a. Hold the right rack-mount bracket against the right rack rail and align the bottom screw hole in the bracket with the marked screw hole on the rail.

b. Insert a screw through the bottom hole in the bracket and finger tighten the screw.

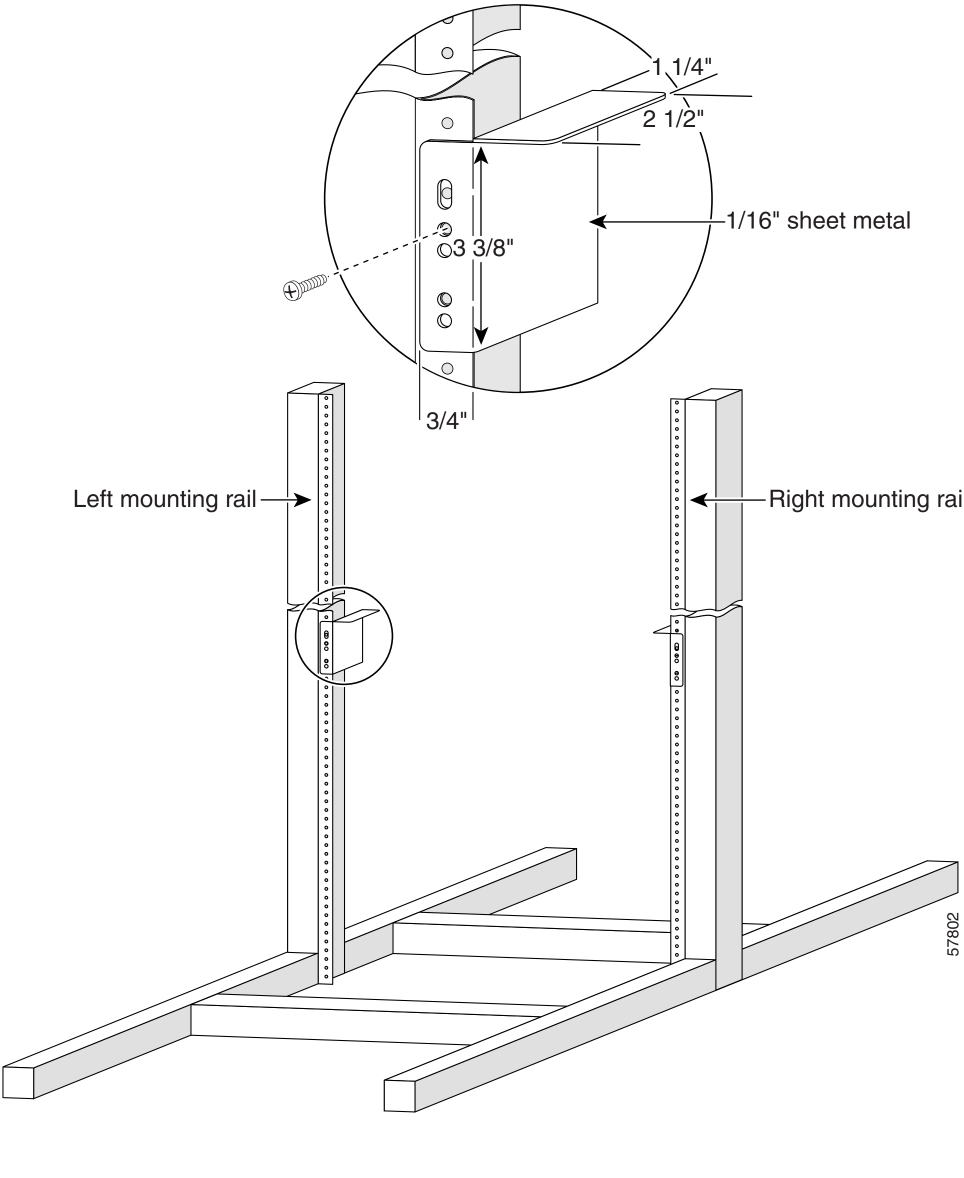
c. Insert and finger tighten a second screw in the top hole in the bracket.

Step 3 Follow Step 2a through Step 2c to mount the left rack-mount bracket.

Step 4 Use a level to verify that the tops of the two brackets are level, or use a measuring tape to verify that both brackets are the same distance from the tops of both rack rails.

Step 5 Use a screwdriver to tighten all the screws.

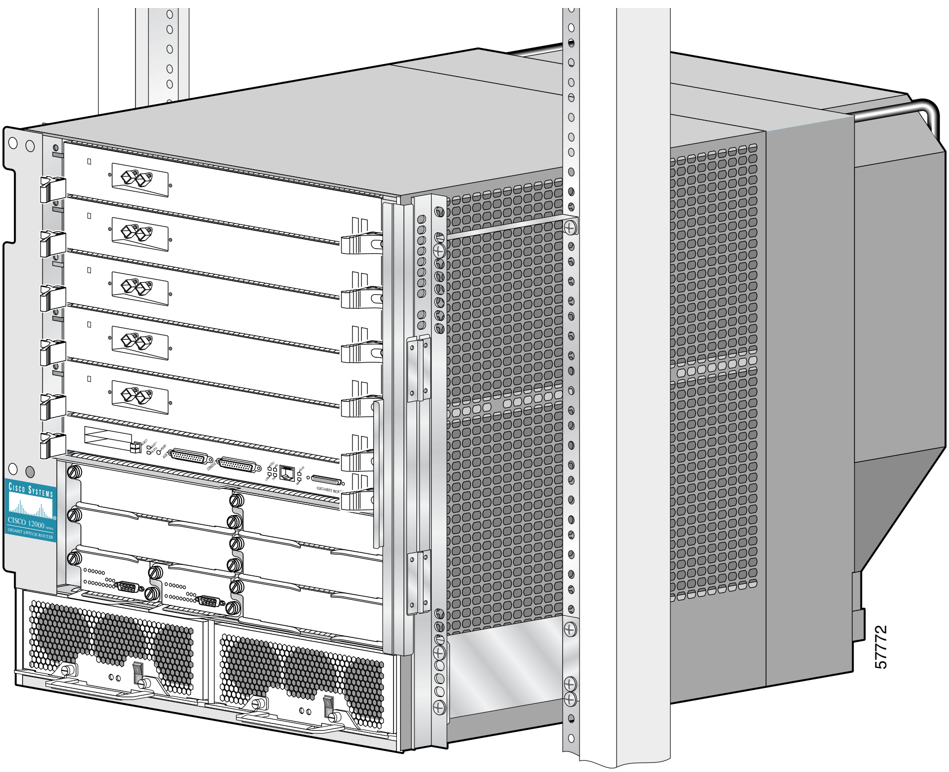
Figure 3-1 Installing the Optional Rack-Mount Brackets



Installing Center-Mount Brackets (Optional)

To install the Cisco 12006 or Cisco 12406 Router in the center-mount position, you must first install the upper and lower center-mount brackets on the equipment rack rails, then secure the chassis to the center-mount brackets. (See Figure 3-2.) If you do not plan to use the optional center-mount brackets, proceed directly to the “Installing the Chassis in a Rack” section on page 3-7.

Figure 3-2 Lower and Upper Center-Mount Brackets



The optional center-mount bracket installation kit ships in an accessories box included in the router shipping container. If any parts are missing, contact a Cisco service representative for assistance.

Tools and Equipment Required

You need the following items to install the optional center-mount rack-mounting brackets:

- Number 2 Phillips screwdriver
- Tape measure (optional)
- Level (optional)

Installing the Optional Center-Mount Brackets

To install the center-mount brackets, see Figure 3-2 and follow these steps:

Step 1 Measure and mark the hole at the same height on both the left and right posts.

Caution When installing the right side lower center-mount bracket, ensure that the bracket does not impede airflow through the air filter, which could cause overheating in the router.

Step 2 Mount the lower right bracket:

a. Hold the lower right bracket against the right rack rail and align the bottom screw hole in the lower bracket with the marked screw hole.

b. Pick a bottom bracket hole that aligns with a hole in the rack rail, then insert a screw in the hole and finger tighten the screw.

c. Insert a second screw in the top hole in the bracket and finger tighten that screw.

Step 3 Repeat Step 2a through Step 2c to mount the lower left center-mount bracket so that it is at the same height as the lower right bracket.

Step 4 Use a level to verify that the tops of the two brackets are level, or use a measuring tape to verify that both brackets are the same distance from the tops of both rack rails.

Step 5 Use a screwdriver to tighten all the screws.

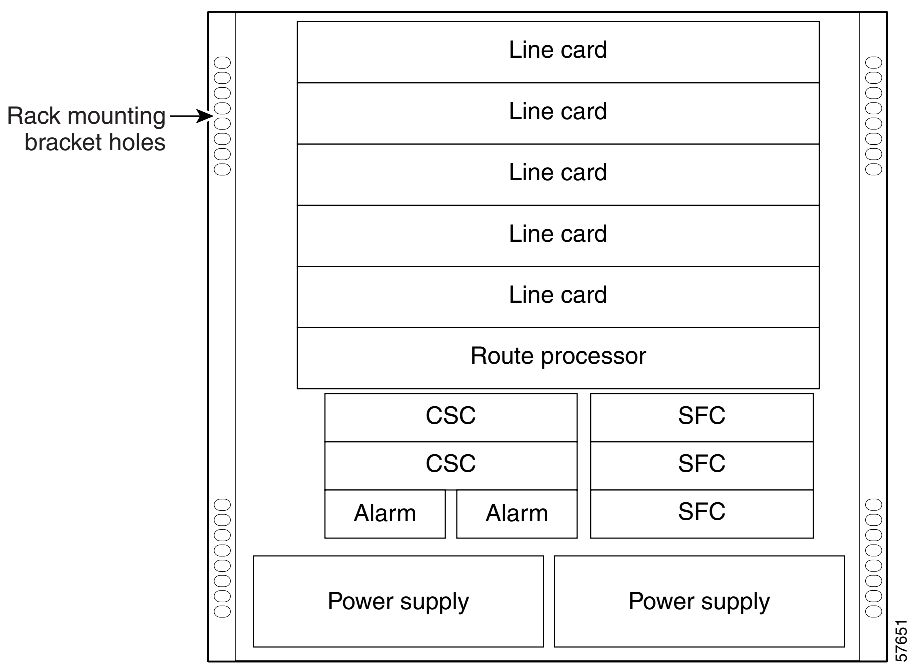
Step 6 Repeat Step 1 through Step 5 for both upper center-mount brackets.

Installing the Chassis in a Rack

This section explains how to install Cisco 12006 and Cisco 12406 Routers in a rack. This procedure assumes you have unpacked the router using the *Cisco 12006 and Cisco 12406 Router Unpacking and Repacking Instructions* (Document number 78-16104-xx) posted on the outside of the shipping container.

You mount the chassis in the equipment rack by setting the chassis in position against the rack rails and then securing it to the rack or optional center-mount brackets with screws through holes in the rack-mounting flanges on either side of the chassis. To accommodate racks with different hole patterns in their rails, the chassis rack-mounting flanges have two groups of eight oblong screw holes on either side. (See Figure 3-3.) The mounting holes in the chassis flanges are spaced so that one mounting hole in each hole group aligns with a hole in the rack rail or optional center-mount bracket. By using the corresponding mounting hole (in the same hole group) on the opposite side of the chassis, you can level the chassis in the rack.

Figure 3-3 Chassis Mounting Bracket Holes



To install the chassis in a rack, see Figure 3-3 and follow these steps:

Step 1 Move the router as close to the installation location as possible without interfering with the installation process.

Step 2 With one person lifting from the front and one from the rear of the chassis, grasp the front and rear of the chassis, lift the chassis off the pallet, and position the chassis in the rack.

Note A third person might be needed to assist in lifting and positioning the chassis in the rack.

Step 3 Install the screws to secure the chassis to the rack:

a. Look at the bottom mounting holes on the chassis rack-mount flanges. Align one of the holes with a mounting hole in the rack.

b. Install one of the mounting screws provided.

c. On the other side of the chassis, adjust the position of the chassis so that the same mounting hole in the bottom group of mounting holes is aligned with a hole in the rack.

d. Install one of the mounting screws provided.

Step 4 Repeat Step 3a through Step 3d for additional mounting holes.

Caution Do not allow the chassis to hang free until you have installed a screw in all four hole groups (at least two screws on each side of the chassis).

Step 5 Use a screwdriver to tighten all the screws.

Installing the Chassis on a Tabletop or Flat Surface

Follow the steps below to install a Cisco 12006 Router or Cisco 12406 Router on a tabletop or stable flat surface. You can use the same mounting hardware that secured your router to the shipping pallet to secure the chassis to a flat surface.

Step 1 Move the router as close to the installation location as possible.

Caution Do not lift the chassis by the blower module handle. This handle is designed to support only the weight of the blower module.

Step 2 With one person positioned at the front of the chassis and one at the rear, lift the chassis off the pallet and position the chassis on the flat surface.

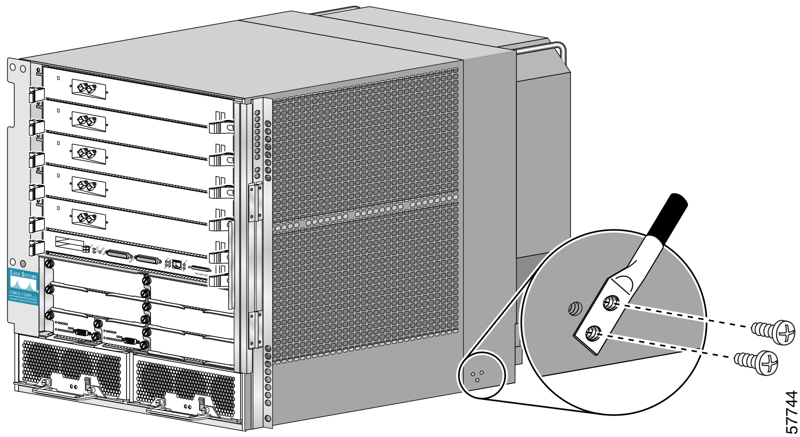
Step 3 Secure the chassis to the flat surface to ensure that it does not fall off.

Supplemental Bonding and Grounding Connections

If the router is installed in a network equipment building system (NEBS) environment, follow the guidelines in this section. For installations other than in a NEBS environment, you may chose to rely on the safety earth ground connection supplied via the International Electrotechnical Commission (IEC) 320 inlets for AC-powered units and the main terminal block ground connection for DC-powered units.

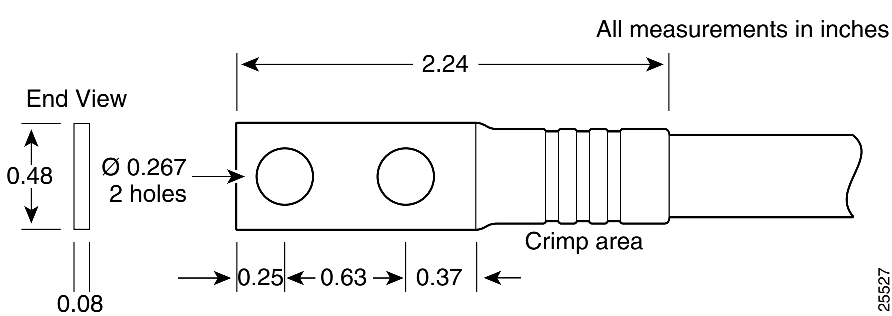
Even though the router chassis requires a safety earth ground connection as part of the power cabling to the PDU, we strongly recommend that you connect the central office ground system or interior equipment grounding system to the supplemental bonding and grounding receptacle on the router chassis, which satisfies the Telcordia NEBS requirement for supplemental bonding and grounding connections. This receptacle consists of three threaded inserts located on the side of the chassis near the back panel. (See Figure 3-4.)

Figure 3-4 Supplemental Bonding and Grounding Port for NEBS Compliance



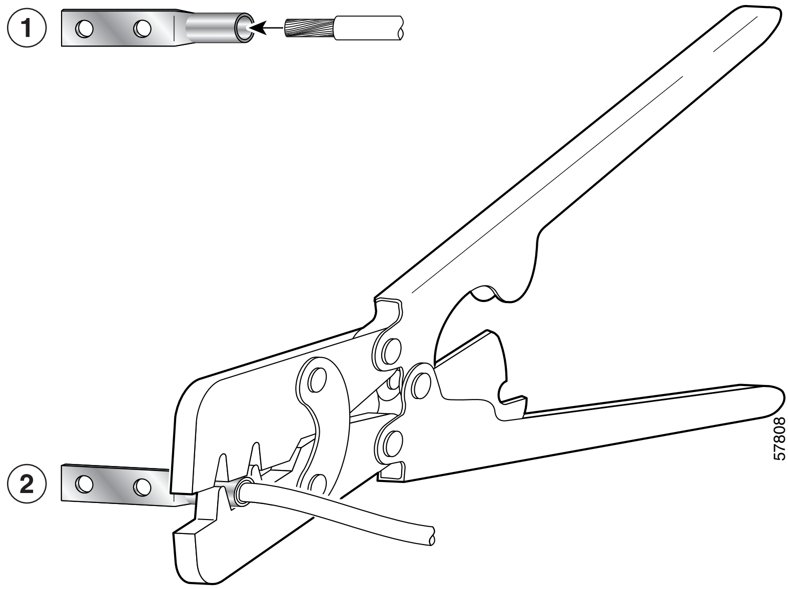
Use a dual-hole lug to connect to the chassis with two 6.3-mm (M6) screws on the 0.63-inch (16-mm) centers as shown in Figure 3-4 and Figure 3-5. The lug can be ordered from Cisco (Part Number 32-0607-01).

Figure 3-5 Cable Lug



The dual-hole lug is crimped onto a grounding wire of a wire size and length determined by your router location and facility environment. The crimping tool shown in Figure 3-6 is a standard crimping tool obtainable from many sources.

Figure 3-6 Crimping the Lug



1	Place ground wire in the lug	**2**	Crimp the lug

Note The three threaded inserts that make up the grounding receptacle are set in a triangle so that you can choose any two of the three holes to attach the lug and grounding cable.

Connecting RP and Line Card Cables

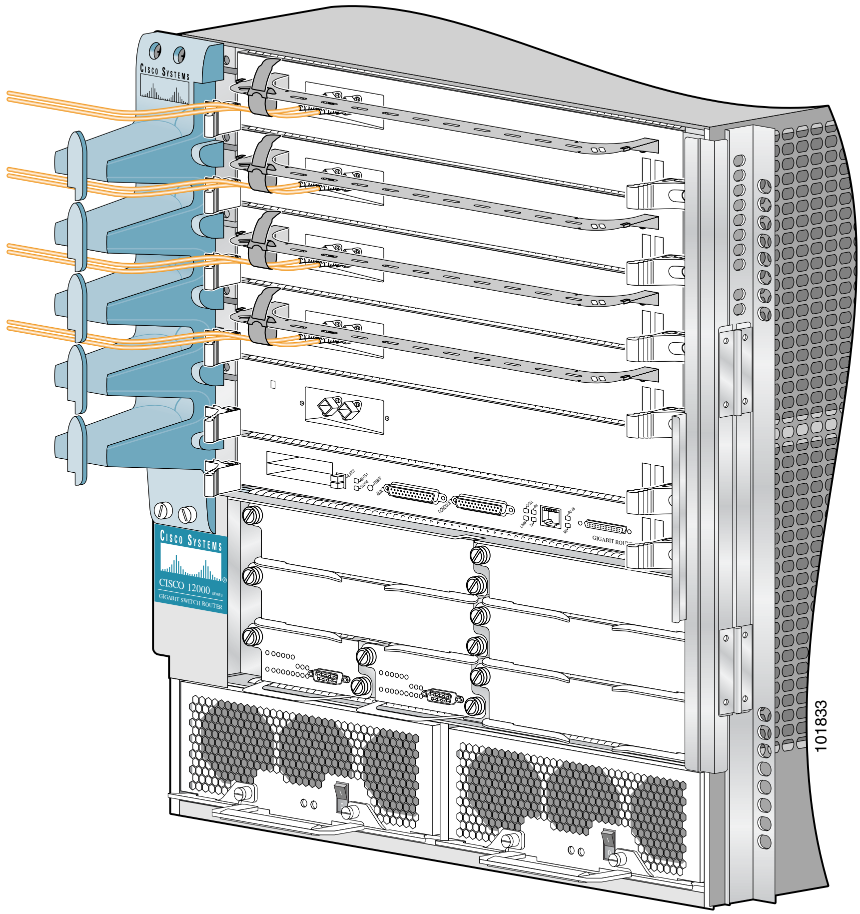
To connect RP and line card cables, see Figure 3-7 and follow these steps:

Step 1 Attach an ESD-preventive strap to your wrist and connect the leash to the chassis or to another grounded, bare metal surface.

Step 2 Proceeding from left to right, identify the cables that attach to the first RP or line card.

Step 3 Carefully route the interface cable through the chassis cable-management bracket and across the card to the card interface port; do this for one cable at a time.

Figure 3-7 Chassis Cable-Management Bracket



Step 4 Proceeding from left to right, identify the cable that connects to each card port and connect the cable to the RP or line card port.

Step 5 Proceeding from left to right, carefully wrap the cables into the line card cable-management bracket using the velcro straps.

Caution Carefully adjust the cable in the cable-management brackets to prevent any kinks or sharp bends in the interface cable. Kinks and sharp bends can destroy or degrade the ability of the optical fiber to propagate the signal-encoded beam of light accurately from one end of the cable to the other. Also, allow adequate strain relief in the interface cable.

Step 6 Route the cable through the fingers on the vertical chassis cable-management bracket and turn the latch on the front of the bracket to secure the cables in the bracket.

Connecting Alarm Card Cables

Cisco 12006 and Cisco 12406 Routers have two alarm cards located in the two slots immediately above the left power supply bay and directly below the clock and scheduler card slots. Each alarm card is equipped with a standard DB-9 connector, labeled ALARM. This connector can be used to connect the router to an external site alarm maintenance system so that any critical, major, and minor alarms generated in the router also energize alarm relays on the alarm card and activate the external site alarm. Appendix A, "Technical Specifications," lists the pin-to-signal correspondence between the connector pins and the alarm card relay contacts.

Because alarm contact cables are entirely dependent on installation site circumstances, alarm connector cables are not available from Cisco Systems.

Note Only safety extra-low voltage (SELV) circuits can be connected to the alarm connector. Maximum rating for the alarm circuit is 2A, 50VA.

Note To comply with Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, you must use a shielded cable when connecting to the external alarm ports on the alarm card. The shielded cable is terminated by shielded connectors on both ends, with the cable shield material tied to both connectors.

Connecting to the Console and Auxiliary Ports

This section provides the information for connecting console terminals and other auxiliary devices to the console and auxiliary ports on the router. Both Data Set Ready (DSR) and Data Carrier Detect (DCD) signals are active when the system is running. The console port does not support modem control or hardware flow control. GRP ports are discussed below. PRP ports are discussed in the "PRP Console and Auxiliary Ports" section on page 3-18.

GRP Console and Auxiliary Ports

This section provides connection equipment and pin designation information for the console and auxiliary ports on the Gigabit Route Processor (GRP).

Note To maintain Class B, EMI compliance, shielded cables must be used on the console and auxiliary ports of the GRP= and GRP-B=.

The GRP has two EIA/TIA-232 ports:

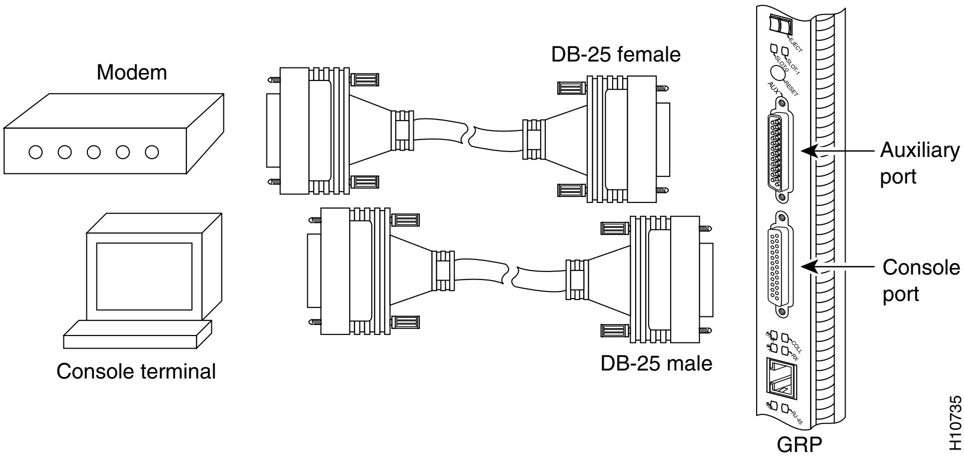
- DCE DB-25 receptacle for connecting a console terminal
- DTE DB-25 plug for connecting other DTE devices

The DCE-mode console port is a DCE DB-25 receptacle used for connecting a console terminal, which you will need to configure the router.

The DTE-mode auxiliary port is a DTE DB-25 plug for connecting a modem or other DCE device (such as a channel service unit/data service unit [CSU/DSU] or another router) to the router.

Note The console and auxiliary ports are asynchronous serial ports; any devices connected to these ports must be capable of asynchronous transmission. Asynchronous is the most common type of serial device; for example, most modems are asynchronous devices.

Figure 3-8 ***GRP Console DCE and Auxiliary DTE Port Connections***



Check your terminal documentation to determine the baud rate of the terminal you plan to use. If your documentation does not specify settings, use the following terminal settings: 9600 baud, 8 data bits, no parity, and 2 stop bits. You will need an EIA/TIA-232 DCE console cable to connect the terminal to the console port.

Note To comply with Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect all console, auxiliary, and Ethernet interfaces only to intrabuilding or nonexposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

GRP Console Port Signals

The console port on the GRP requires a straight-through EIA/TIA-232 cable. Table 3-1 lists the signal-to-pin correspondence for the GRP console port.

Table 3-1 GRP Console Port Pin Signals

Pin	Signal	Input/Output	Description
1	GND	–	Ground
2	TxD	Output	Transmit Data
3	RxD	Input	Receive Data
6	DSR	Input	Data Set Ready (always on)
7	GND	–	Ground
8	DCD	Input	Data Carrier Detect (always on)
20	DTR	Output	Data Terminal Ready

GRP Auxiliary Port Signals

The GRP auxiliary port is a DB-25 plug DTE port for connecting a modem or other DCE device (such as a CSU/DSU or other router) to the router. The auxiliary port is located next to the console port on the GRP card. The auxiliary port supports hardware flow control and modem control. An example of a modem connection is shown in Figure 3-8. Table 3-2 lists the signal-to-pin correspondence for the auxiliary port.

Note To maintain Class B EMI compliance, shielded cables must be used on the console and auxiliary ports of the GRP= and GRP-B=.

Table 3-2 GRP Auxiliary Port Signals

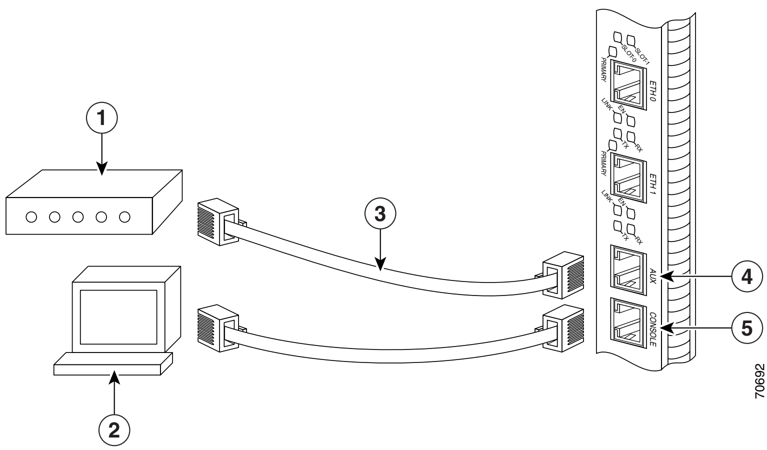
Pin	Signal	Input/Output	Description
1	Signal Ground	–	Signal Ground
2	TxD	Input	Transmit Data
3	RxD	Output	Receive Data
4	RTS	Input	Request To Send (used for hardware flow control)
5	CTS	Output	Clear To Send (used for hardware flow control)
6	DSR	Output	Data Set Ready
7	Signal Ground	–	Signal Ground
8	CD	Output	Carrier Detect (used for modem control)
20	DTR	Input	Data Terminal Ready (used for modem control only)
22	RING	Output	Ring

PRP Console and Auxiliary Ports

The system console port on the PRP is a DCE RJ-45 receptacle for connecting a data terminal, which you must configure. The console port is labeled *Console*, as shown in Figure 3-9. Before connecting the console port, check the documentation for your terminal to determine the baud rate.

If your documentation does not specify settings, use the following terminal settings: 9600 baud, 8 data bits, no parity, and 2 stop bits. The console port requires a rollover RJ-45 cable.

Figure 3-9 PRP Console and Auxiliary Port Connections



1	Modem	**4**	Auxiliary port
2	Console terminal	**5**	Console port
3	RJ-45 Ethernet cables	**–**	—

Note The console and auxiliary ports are both asynchronous serial ports; any devices connected to these ports must be capable of asynchronous transmission. Asynchronous is the most common type of serial device; for example, most modems are asynchronous devices.

Caution The ports labeled Ethernet, 10BASE-T, Token Ring, Console, and AUX are safety extra-low voltage (SELV) circuits. SELV circuits should only be connected to other SELV circuits.

Note RP cables are not available from Cisco, but are available from any commercial cable vendor.

Note To comply with Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect all console, auxiliary, Ethernet, and BITS (PRP2) interfaces only to intrabuilding or nonexposed wiring or cabling. The intrabuilding cable must be shielded and the shield must be grounded at both ends.

PRP Console Port Signals

The console port on the PRP is a DCE RJ-45 receptacle. Table 3-3 lists the signal-to-pin correspondence for the PRP console port.

Table 3-3 PRP Console Port Signals

Console Port Pin	Signal	Input/Output	Description
1[1]	—	—	—
2	DTR	Output	Data Terminal Ready
3	TxD	Output	Transmit Data
4	GND	—	Signal Ground
5	GND	—	Signal Ground
6	RxD	Input	Receive Data
7	DSR	Input	Data Set Ready
8[1]	—	—	—

1. These pins are not connected.

PRP Auxiliary Port Signals

The auxiliary port on the PRP is a DTE, RJ-45 plug for connecting a modem or other DCE device (such as a CSU/DSU or another router) to the router. The port is labeled *AUX*, as shown in Figure 3-9. The asynchronous auxiliary port supports hardware flow control and modem control. Table 3-4 lists the signal-to-pin correspondence for the PRP auxiliary port.

Table 3-4 PRP Auxiliary Port Signals

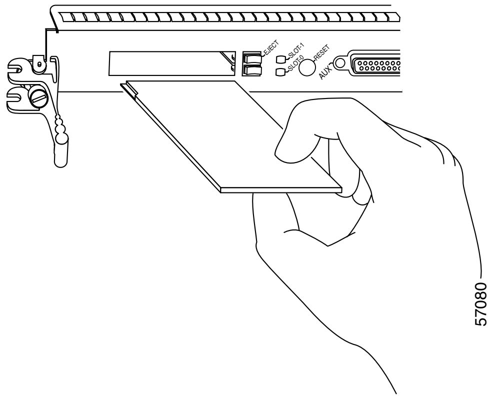
Auxiliary Port Pin	Signal	Input/Output	Description
1	RTS	Output	Request To Send
2	DTR	Output	Data Terminal Ready
3	TxD	Output	Transmit Data
4	GND	—	Signal Ground
5	GND	—	Signal Ground
6	RxD	Input	Receive Data
7	DSR	Input	Data Set Ready
8	CTS	Input	Clear To Send

Installing a Flash Memory Card

By default, a Flash memory card containing a valid Cisco IOS software image is inserted in PCMCIA slot 0 before the router is shipped. (See Figure 3-10.) PCMCIA slot 0 (SLOT-0) is the bottom slot and slot 1 (SLOT-1) is the top slot. Both Flash memory card slots on each RP can be used at the same time.

The software configuration register is set to 0x0102, which causes the router to boot automatically from the Cisco IOS software image stored on the Flash memory card.

Figure 3-10 Flash Memory Card Slot Opening

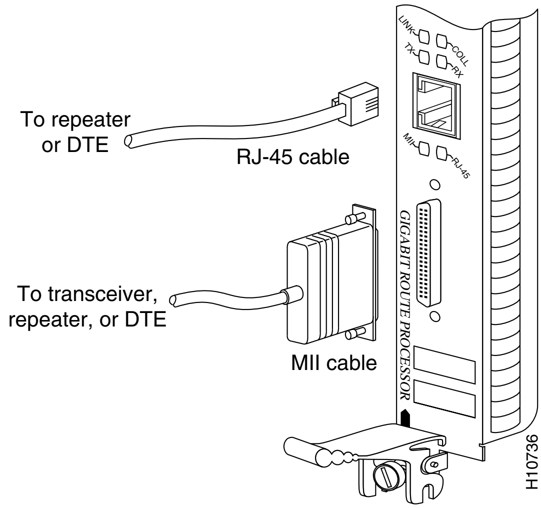


Ensure that a console terminal is connected to the RP console port and turned on, or that you have a remote login to the router from another device through a Telnet session.

Connecting the GRP to an Ethernet Network

This section provides information for connecting the GRP to an Ethernet network. Figure 3-11 shows the RJ-45 and MII Ethernet ports on the GRP.

Figure 3-11 RJ-45 and MII Ethernet Connections



The GRP has one Ethernet port, which uses either of these port connectors:

- RJ-45 receptacle—An 8-pin media-dependent interface (MDI) RJ-45 receptacle for either an IEEE 802.3 10BASE-T (10 Mbps) or an IEEE 802.3u 100BASE-TX (100 Mbps) connection.
- MII receptacle—A 40-pin media independent interface (MII) receptacle that provides additional flexibility in Ethernet connections. This connector can also be used for either an IEEE 802.3 10BASE-T (10 Mbps) or an IEEE 802.3u 100BASE-TX (100 Mbps) connection.

Note The RJ-45 and MII receptacles on the GRP represent two physical connection options for one Ethernet interface; you can use either the MDI RJ-45 connection or the MII connection, but not both simultaneously. The transmission speed of the Ethernet port is set through an auto-sensing scheme on the GRP.
The speed is determined by the network to which the Ethernet interface is connected, and is not user-configurable. Moreover, even at the auto-sensed data transmission rate of 100 Mbps, the Ethernet port provides maximum usable bandwidth of less than 100 Mbps. Expect a maximum usable bandwidth of approximately 20 Mbps when using either the MII or RJ-45 connection.

The Ethernet port can use either unshielded twisted-pair or screened twisted-pair cable. In sites where extremely high immunity to noise is required, screened twisted-pair cable is recommended. Figure 3-12 shows the layout of the Ethernet MII receptacle on the GRP.

Figure 3-12 Ethernet MII Receptacle

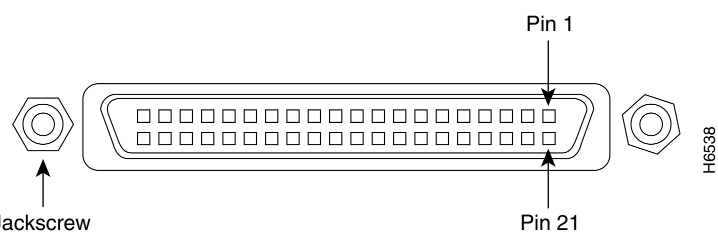


Table 3-5 lists the signal-to-pin correspondence for the Ethernet MII connector.

Table 3-5 Ethernet MII Pin Configuration

Pin[1]	In	Out	Input/Output	Description	Code
14 to17	–	Yes	–	Transmit Data	TxD
12	Yes	–	–	Transmit Clock	Tx_CLK[2]
11	–	Yes	–	Transmit Error	Tx_ER
13	–	Yes	–	Transmit Enable	Tx_EN
3	–	Yes	–	MII Data Clock	MDC
4 to 7	Yes	–	–	Receive Data	RxD

Table 3-5 Ethernet MII Pin Configuration (continued)

Pin[1]	In	Out	Input/Output	Description	Code
9	Yes	–	–	Receive Clock	Rx_CLK
10	Yes	–	–	Receive Error	Rx_ER
8	Yes	–	–	Receive Data Valid	Rx_DV
18	Yes	–	–	Collision	COL
19	Yes	–	–	Carrier Sense	CRS
2	–	–	Yes	MII Data Input/Output	MDIO
22 to 39	–	–	–	Common	Ground
1, 20, 21, 40	–	–	–	+5.0 V	V

1. Unlisted pins are not used.
2. Tx_CLK and Rx_CLK are provided by the external transceiver.

Figure 3-13 shows the pin configuration on the Ethernet RJ-45 receptacle on the GRP. Table 3-6 lists the signal-to-pin correspondence for the Ethernet RJ-45 receptacle on the GRP.

Figure 3-13 Ethernet RJ-45 Receptacle

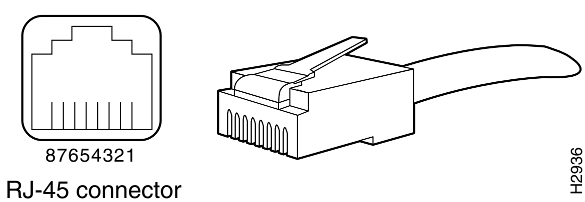


Table 3-6 Ethernet RJ-45 Receptacle Pin Configuration

Pin	Signal
1	TX+
2	TX–
3	RX+

Table 3-6 Ethernet RJ-45 Receptacle Pin Configuration (continued)

Pin	Signal
4	Termination Network
5	Termination Network
6	RX–
7	Termination Network
8	Termination Network

Warning **The ports labeled Ethernet, 10BASE-T, Token Ring, Console, and AUX are safety extra-low voltage (SELV) circuits. SELV circuits should only be connected to other SELV circuits. Because the basic rate interface (BRI) circuits are treated like telephone network voltage, avoid connecting the SELV circuit to the telephone network voltage (TNV) circuits.**

Connecting the PRP to an Ethernet Network

This section provides information for connecting the PRP on your router to an Ethernet network.

The PRP includes two 10/100 Mbps Ethernet ports, each using an 8-pin RJ-45 receptacle for either IEEE 802.3 10BASE-T (10 Mbps) or IEEE 802.3u 100BASE-TX (100 Mbps) connections. The transmission speed of the Ethernet ports is auto-sensing by default and is user configurable.

The Ethernet interfaces on the PRP are end-station devices, not repeaters; therefore, you *must* connect an Ethernet interface to a repeater or hub. To connect cables to the PRP Ethernet interfaces (ports labeled ETH0 and ETH1), attach the Category 5 UTP cable directly to a RJ-45 receptacle on the PRP.

RJ-45 cables are not available from Cisco Systems, but are available from outside commercial cable vendors.

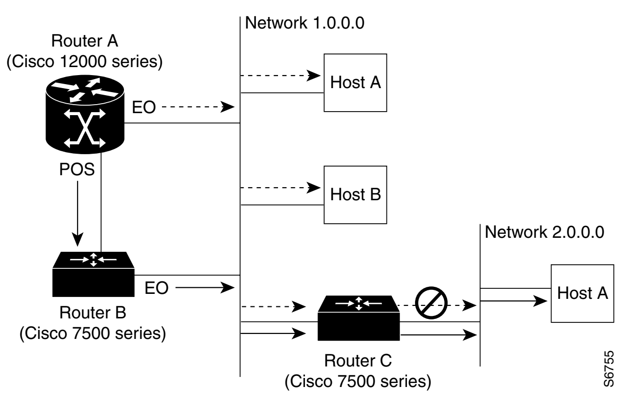
Note Use cables that comply with EIA/TIA-568 standards. (See Table 3-8 on page 3-29 and Table 3-9 on page 3-29 for cable recommendations and specifications.)

Caution The Ethernet ports are used primarily as Telnet ports into the router, and for booting or accessing Cisco IOS software images over a network to which an Ethernet port is directly connected. Cisco Express Forwarding (CEF) functions are switched off by default for security reasons. Cisco strongly cautions you to consider the security implications of switching on CEF routing functions on these ports.

Figure 3-14 shows an example of the functionality of an Ethernet port. In this example, you cannot access Network 2.0.0.0 via the Ethernet port (ETH0) on the PRP in Router A; you can only access the hosts and Router C, which are in Network 1.0.0.0. (See dotted arrows in Figure 3-14.)

To access Network 2.0.0.0 from Router A, use an interface port on one of the line cards (in this example, a Packet-over-SONET [POS] line card in Router A) to go through Router B, through Router C, and into Network 2.0.0.0. (See solid arrows in Figure 3-14.)

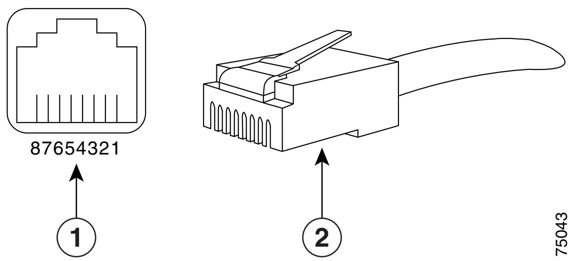
Figure 3-14 Using the Ethernet Port on the PRP



PRP Ethernet Connections

Figure 3-15 shows a PRP RJ-45 receptacle and cable connector. The RJ-45 connection does not require an external transceiver. The RJ-45 connection requires Category 5 unshielded twisted-pair (UTP) cables, which are not available from Cisco Systems, but are available from commercial cable vendors. Table 3-7 lists the signal-to-pin correspondence for the RJ-45 receptacle.

Figure 3-15 RJ-45 Receptacle and Plug (Horizontal Orientation)



1	RJ-45 receptacle	**2**	Category 5 UTP cable with plug

Warning **The ports labeled Ethernet, 10BASE-T, Token Ring, Console, and AUX are safety extra-low voltage (SELV) circuits. SELV circuits should only be connected to other SELV circuits. Because the BRI circuits are treated like telephone network voltage, avoid connecting the SELV circuit to the telephone network voltage (TNV) circuits.**

Table 3-7 PRP RJ-45 Ethernet Receptacle Pinout

Ethernet Port Pin	Signal	Description
1	TxD+	Transmit data +
2	TxD–	Transmit data –
3	RxD+	Receive data +
4	Termination Network	No connection
5	Termination Network	No connection

Table 3-7 PRP RJ-45 Ethernet Receptacle Pinout (continued)

Ethernet Port Pin	Signal	Description
6	RxD–	Receive data –
7	Termination Network	No connection
8	Termination Network	No connection

Depending on your RJ-45 cabling requirements, use the connector pinouts shown in Figure 3-16 or Figure 3-17.

Figure 3-16 Straight-Through Cable Pinout (Connecting MDI Ethernet Port to MDI-X Wiring)

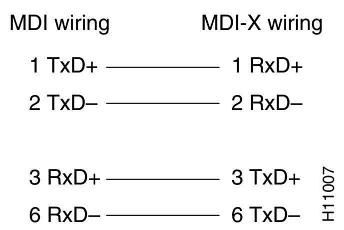


Figure 3-17 Crossover Cable Pinout (for Connecting Two PRPs)

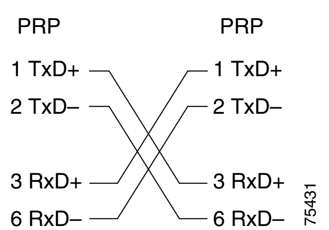


Table 3-8 lists the cabling specifications for 100-Mbps transmission over unshielded twisted-pair (UTP) cables.

Note The transmission speed of the Ethernet ports is auto-sensing by default and is user configurable.

Table 3-8 Specifications and Connection Limits for 100-Mbps Transmission

Parameter	RJ-45
Cable specification	Category 5[1] UTP, 22 to 24 AWG[2]
Cable length (max)	—
Segment length (max)	328 feet (100 m) for 100BASE-TX
Network length (max)	656 feet (200 m)[3] (with 1 repeater)

1. EIA/TIA-568- or EIA-TIA-568 TSB-36-compliant. Not supplied by Cisco.
2. AWG = American Wire Gauge. This gauge is specified by the EIA/TIA-568 standard.
3. This length is specifically between any two stations on a repeated segment.

Table 3-9 lists IEEE 802.3u physical characteristics for 100BASE-TX.

Table 3-9 IEEE 802.3u Physical Characteristics

Parameter	100BASE-TX
Data rate (Mbps)	100
Signaling method	Baseband
Maximum segment length	100 m between DTE[1] and repeaters
Media	Category 5 UTP (for RJ-45)
Topology	Star/Hub

1. DTE = data terminal equipment.

Connecting to an AC Power Source

This section presents the procedure for connecting your router to an AC power source. A power factor corrector (PFC) allows the AC-input power supply to accept AC power source voltage from an AC power source operating between 100 and 240 VAC, 20-Amp service in North America; and a range of from 185 to 264 VAC, 16-Amp service in an international environment.

Caution The AC-input power supply weighs 14 pounds (6.4 kilograms). Use two hands when handling a power supply.

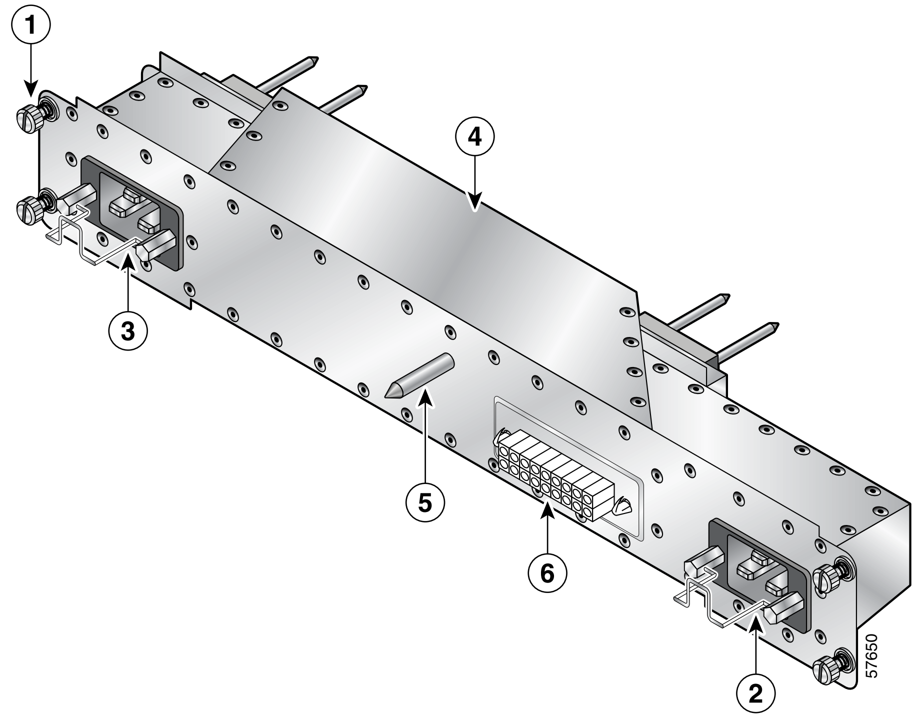
Warning **The AC-input power supply power standby switch should be in the OFF position.**

When operating your router on a power source, the power supply bays must have one of the following power combinations installed before operating the router:

Table 3-10 Required Power Combinations

Router Power	Combination
AC power	1 AC-input power supply 1 power supply blank
	2 AC-input power supplies
DC power	1 DC-input PEM 1 PEM blank
	2 DC-input PEMs

Figure 3-18 AC Power Distribution Unit



1	Captive screws (four)	**4**	AC power distribution unit
2	AC power cord receptacle A	**5**	Guide pin
3	AC power cord receptacle B	**6**	Blower module connector

To connect AC power to the AC PDU on the router, see Figure 3-18 and follow these steps:

Step 1 Attach an ESD-preventive strap to your wrist and connect the leash to the chassis or to another grounded, bare metal surface.

Step 2 Locate the two AC power cords and remove them from their shipping packaging. Verify that the AC power cords shipped with the power supplies are the correct type for your site.

Note If you have received the wrong type of AC power cord, contact your service representative for a replacement.

Step 3 Plug the socket end of each AC power cord into a receptacle on the PDU. (See Figure 3-18.)

Step 4 Insert the plug end of each AC power cord into the AC power source outlet.

For full redundancy, connect each AC-input power supply to an independent power circuit with its own circuit breaker. We also recommend that you use an uninterruptable power source (UPS) to protect against power failures at your site.

Step 5 Verify that the AC power source circuit breaker servicing each of the AC-input power supplies is switched on.

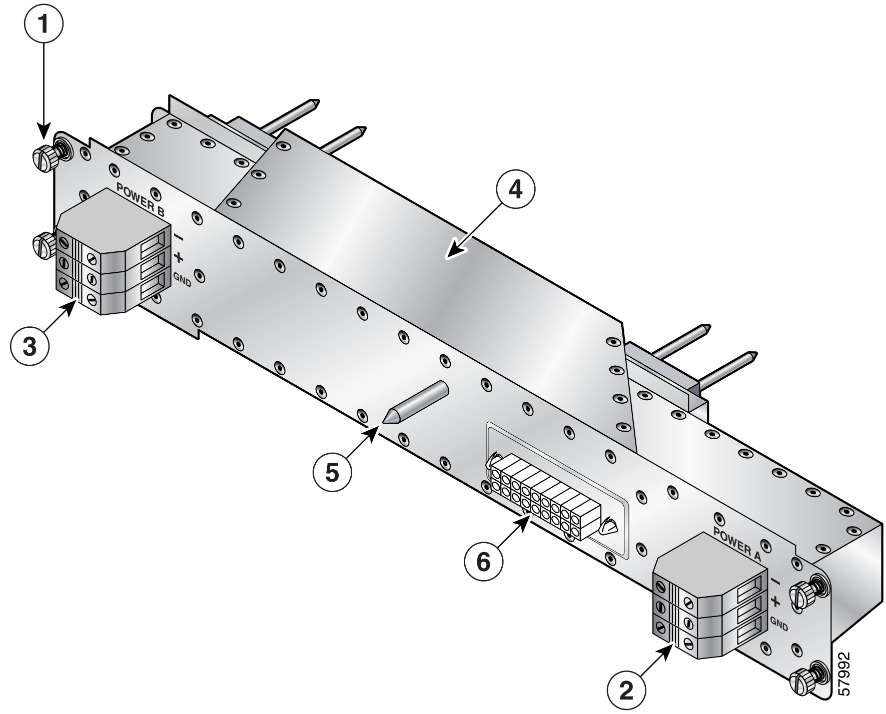
Note When operating your router on a single power module, the second power module bay must have a blank filler (MAS-GSR-PWRBLANK=) installed to ensure EMI compliance.

Connecting to a DC Power Source

This section provides the procedure for connecting the router to a DC power source.

Warning **The circuit breaker switch on the faceplate of the DC-input PEM should be in the OFF position.**

Figure 3-19 DC PDU



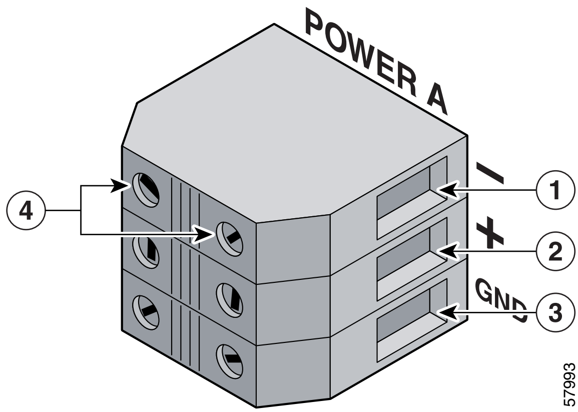
1	Captive screws (four)	**4**	DC PDU
2	DC power connector block (A)	**5**	Guide pin
3	DC power connector block (B)	**6**	Blower module connector

To connect source DC power to the DC PDU, see Figure 3-19 and Figure 3-20 and follow these steps:

Step 1 Attach an ESD-preventive strap to your wrist and connect the leash to the chassis or to another grounded, bare metal surface.

Step 2 Locate the DC PDU on the back of the router. The PDU is positioned directly below and behind the blower module.

Figure 3-20 DC PDU Power Connector Block



1	Negative terminal port	**3**	Ground terminal port
2	Positive terminal port	**4**	Terminal port connector screws

Step 3 Connect the source DC power leads to the three terminal ports in the DC power connector block (see Figure 3-20) in this order:

- Ground lead first (bottom port on the connector block)
- Positive lead second (middle port on the connector block)
- Negative lead last (top port on the connector block)

a. Push the lead into the connector block port.

b. Use a flat-blade screwdriver to tighten the set screw and secure the lead.

c. Repeat Step 3a and Step 3b for the remaining leads and for the second PDU connector block.

Step 4 Verify that the source DC circuit breaker servicing the DC PDU is switched on.

Power On the Router

To power on the router, follow these steps:

Step 1 Either switch on all the circuit breakers or plug the power cord into an active power source that controls power to the PDU in the router.

During the first-time startup, the system displays the system banner information. Check the startup banner and displays to ensure that the system has restarted properly and that all the interfaces reinitialize properly.

Step 2 Check the power module LEDs. They should appear as described below:

- For a router equipped with AC-input power supplies:
  - Green LED labeled AC—When the power module is fully seated in its bay and is receiving source power within the required range, this LED should be on. It indicates that AC power is present and is within specified limits. The power supply fan should also be on.
  - Green LED labeled DC—Power supply is operating normally in a powered-on condition.
- For a router equipped with DC-input PEMs:
  - Green LED labeled INPUT OK—When the power module is fully seated in its bay and is receiving source power within the required range, this LED should be on. It indicates that DC power is present and is within specified limits. The power supply fan should also be on.
  - Green LED labeled OUTPUT OK—DC-input PEM is operating normally in a powered-on condition.
  - Amber LED labeled MISWIRE—Should be off. When it is on, it indicates that the input is wired backward at the PDU input.

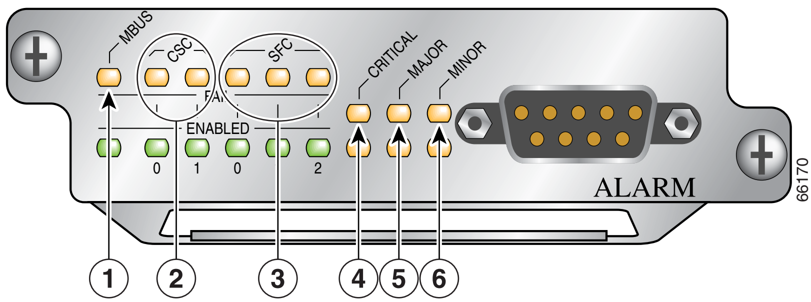
Step 3 Go to the rear of the chassis and visually check the two LEDs on the front of the blower module. They should appear as described below:

- Green LED labeled OK—Should be on
- Red LED labeled FAIL—Should be off

Step 4 Listen for the blowers in the blower module; you should immediately hear them operating.

Note In a noisy environment, the blowers might be difficult to hear; in that case, place your hand in front of the exhaust vents at the rear of the chassis to verify that the blowers are operating.

Figure 3-21 Alarm Card LEDs On/Off Conditions



1	MBus status LED	**4**	Critical alarm LED
2	CSC status LEDs (two)	**5**	Major alarm LED
3	SFC status LEDs (three)	**6**	Minor alarm LED

Step 5 Visually check the LEDs on the two alarm cards. (See Figure 3-21.) When the system is operating correctly, the following LED conditions should be true.

LEDs that normally should be off:

- One MBUS status LED labeled FAIL
- Two CSC status LEDs labeled FAIL
- Three SFC status LEDs labeled FAIL
- Three router alarm LEDs labeled CRITICAL, MAJOR, MINOR

LEDs that normally should be on:

- One MBUS status LED labeled ENABLED
- Two CSC status LEDs labeled ENABLED
- Three SFC status LEDs labeled ENABLED

Step 6 On the console terminal, verify that the console displays the system banner and that the system and all interfaces initialize successfully.

If the power modules do not power up, or if the system or any interfaces do not initialize properly, see Chapter 4, "Troubleshooting the Installation." If you are still unable to resolve the problem, contact your Cisco service representative for assistance.

IOS Software Configuration for the Router

This section explains how to configure your system so that it can access the network or enable other hosts on the network to access your system remotely by means of a Telnet connection. You can find more information in the configuration publications listed in the "If You Need More Information" section on page 3-82.

The system startup process and a procedure for performing a basic configuration of your router are presented in the following sections:

Cisco IOS Software Images

A default Cisco IOS software image for your system is available through any of the internal or external sources described in Table 3-11.

Table 3-11 Cisco IOS Software Image Sources

Onboard Flash Memory on the Gigabit Route Processor (GRP)	The latest Cisco IOS software image is loaded into the Flash memory, a single inline memory module (SIMM) that is preloaded at the factory before the router is shipped. The Flash memory SIMM is also referred to as nonvolatile random access memory (NVRAM). This type of memory retains its contents when system power is off.
Flash Memory Card	A Flash memory card inserted in a PCMCIA slot on the GRP, and loaded with the default software image, can serve as an external storage medium for the default Cisco IOS software image shipped with your router.
TFTP Server	You can download and store a valid Cisco IOS software image via a Trivial File Transfer Protocol (TFTP) using a Telnet connection.

Conditions to Check Before System Startup

Ensure that the following conditions are met before starting up the router:

- All cards are completely inserted into their card cage slots
- All captive screws are tightened
- All interface cable connections are secure
- All the power source cables are secured to the PDU
- All power cables are connected to the appropriate power source
- A terminal device is connected, powered on, and configured to 9600 bps, 8 data bits, no parity, and 2 stop bits (9600,8N2)
- A Flash memory card containing a valid Cisco IOS software image is inserted in PCMCIA slot 0 (zero)

By default, the software configuration register is set to 0x0102, causing the system to boot automatically from the Cisco IOS software image stored on the Flash memory card. New Flash memory cards must be formatted before use. To format a new Flash memory card, refer to the section “Formatting a Flash Memory Card, page 3-67”.

Overview of the Boot Process

The example below assumes that the router is plugged into a power source and the router is running, blower module fans are audible, and alarm card ENABLED LEDs are lit up.

The following is an example of a typical boot process:

- The RP MBus module receives the correct DC voltage and starts executing MBus software.
- The RP determines the router configuration by sending a message via the alarm card requesting all installed devices to identify themselves. Their responses provide slot numbers and card and component types. The RP, line cards, CSCs, and SFCs are then powered up.
- The power-on-reset logic of the RP is delayed long enough to allow power and both local and CSC clocks to stabilize.
- After the power-on reset logic is released, the RP begins to execute the ROM monitor software.
- If the ROM monitor is configured to autoboot, it automatically loads and boots the Cisco IOS software.
- If the ROM monitor is not configured to autoboot, boot the Cisco IOS software manually. See the “Manually Booting the System” section on page 3-47.
- When the Cisco IOS software boots, it polls all other cards in the system, powers them up, and loads the Cisco IOS software they require.

Starting the Router and Observing Initial Conditions

Observe the following conditions the first time you start your router:

- Power cables to the PDU are fully connected to both the PDU and the power source, and are secured with appropriate strain relief.
- Empty card slots or card bays are filled with card blanks. This ensures proper air flow through the chassis and electromagnetic compatibility (EMC).
- All cards are fully inserted in their cages and bays.
- All captive screws are tightened.

- Line card cable-management brackets are attached to their respective line cards.
- Interface cables are completely seated in their line card connectors.
- Interface cables are routed neatly through the chassis cable-management bracket.

Caution Do not overtighten the captive screws on the cards; you might strip the threads on the screw or in the insert in the component faceplate.

- Power modules are fully inserted in their bays and the ejector levers are completely closed and secured.
- Check the power module LEDs:

  For a router equipped with AC-input power supplies, when a power supply is seated in its bay and is receiving the required power source:

  - The green LED labeled AC should be on. It indicates that AC power source is present and is within specified limits.
  - The green LED labeled DC should be on. It indicates that the power supply is operating normally in a powered-on condition.

  For a router equipped with DC-input PEMs—When a PEM is seated in its bay and is receiving the required power source:

  - The green LED labeled INPUT OK should be on. It indicates that DC power source is present and is within specified limits.
  - The green LED labeled OUTPUT OK should be on. It indicates that the PEM is operating normally in a powered-on condition.
  - The amber LED labeled MISWIRE should be off. When it is on, it indicates that the input is wired backward at the PDU input.
- Each power module fan should also be on.

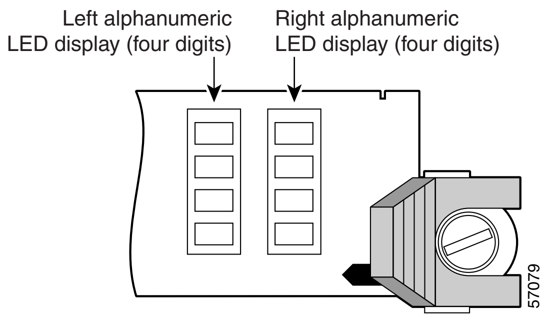
At the rear of the chassis, observe the status of the two LEDs on the blower module. When the blower module is operating correctly, the left LED should should be on (green) and the right LED (red) should be off.

Listen for the blowers in the blower module; they should be running. In a noisy environment, the blower might be difficult to hear. In that case, place your hand near the exhaust vents at the top and bottom rear of the chassis to verify that the blower is operating.

RP Alphanumeric LED

RP alphanumeric LEDs are located at one end of the RP faceplate, near the ejector lever. Figure 3-22 shows the RP LED displays.

Figure 3-22 RP Alphanumeric LED Displays



Each four-digit display shows part of a two-line system message. During the RP boot process, the LED displays present a sequence of messages similar to that shown in Table 3-12.

Table 3-12 LED Display Meaning and Signal Source

LED Display	Meaning	Source
MROM *nnnn*	The MBus microcode begins to execute; *nnnn* is the microcode version number. For example, microcode version 1.17 displays as 0117.[1] Note This display might not be visible because it occurs for only a brief time.	MBus controller
LMEM TEST	Low memory on the RP is being tested.	RP ROM monitor
MEM INIT	The size of main memory on the RP is being discovered.	RP ROM monitor
RP RDY	The system is operational and ready to execute basic Cisco IOS software commands at the ROM monitor prompt (`rommon>`).	RP ROM monitor

Table 3-12 LED Display Meaning and Signal Source (continued)

LED Display	Meaning	Source
RP UP	A valid Cisco IOS image is running.	RP IOS software
PRI RP	The RP is enabled and recognized as the system primary. A valid Cisco IOS image is running.	RP IOS software
SEC RP	The RP is enabled and recognized as the system secondary. A valid Cisco IOS image is running.	RP IOS software

1. The version of MBus microcode running on your system might be different.

RP Interfaces Using the RP LEDs

Two types of RPs are available for Cisco 12006 and Cisco 12406 Routers: the Gigabit Route Processor (GRP) and the Performance Route Processor (PRP).

Each of these route processor types is reviewed in the following sections:

- GRP Interfaces Using the GRP LEDs, page 3-43
- PRP Interfaces Using the PRP LEDs, page 3-44

Note When not explicitly specified, this publication uses the term route processor (RP) to indicate either the GRP or the PRP.

The RJ-45 port LEDs on the RP indicate the following conditions:

- System and RP status
- Which Flash memory card slot is active
- Which Ethernet connection is in use
- What is occurring on the Ethernet interface

The alphanumeric LED displays indicate a successful RP boot.

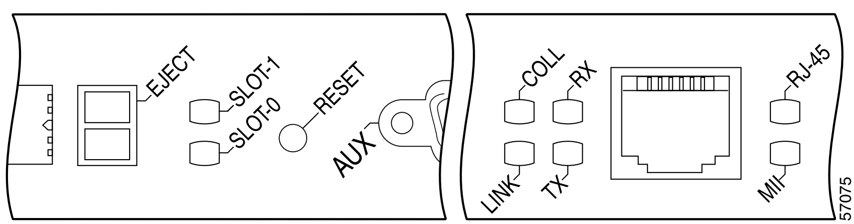
GRP Interfaces Using the GRP LEDs

The GRP faceplate has eight device or port LED activity indicators. Each LED goes on when its corresponding PCMCIA slot is accessed. The ports are as follows:

- Two PCMCIA slot activity LEDs labeled SLOT-0 and SLOT-1.
- Four RJ-45 Ethernet port activity LEDs. These LEDs are used only by the RJ-45 Ethernet connector, and are disabled when the MII Ethernet port is in use.
- Two Ethernet port-selection LEDs labeled MII and RJ-45.

When the Ethernet port LEDs are lit, they identify which of the two Ethernet connections is selected. When the RJ-45 port is selected, that LED is on and the MII LED is off. When the MII port is selected, that LED is on and the RJ-45 LED is off. (See Figure 3-23.)

Figure 3-23 RP RJ-45 and MII Ports LEDs



LINK	Indicates link activity
COLL	Indicates collision detection
TX	Indicates data transmission
RX	Indicates data reception

When you start an unconfigured system for the first time, the console screen displays a system banner and then automatically starts the System Configuration Dialogue. Observe the Cisco IOS banner on the console screen. If a Flash memory card containing a valid Cisco IOS software image is inserted in PCMCIA slot 0 and the software configuration register is set to 0x0102 (the factory default setting), the router automatically boots using this image.

As the router boots the Cisco IOS software image, the console screen displays a system banner similar to the following:

```
Cisco Internetwork Operating System Software
IOS (tm) GS Software (GSR-P-M)
12.0(20020120:204554)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Sat 20-Aug-01 18:34
.
.
.
```

Note The system banner that appears depends on the image version of the Cisco IOS software that the system is running.

If the ROM monitor prompt (`rommon>`) appears on the system console, your router did not find a valid system image, or the boot sequence was otherwise interrupted, and the system entered read-only memory (ROM) monitor mode.

To boot a Cisco IOS software image manually, enter the **boot** command on the system console. For information on using the various forms of the **boot** command, see the following sections:

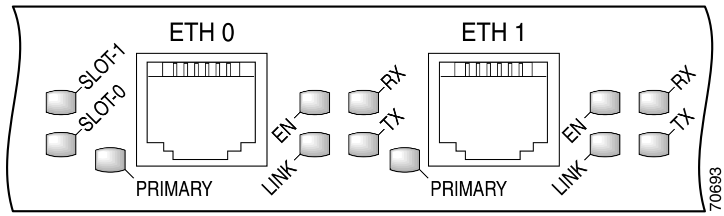
- Locating a Valid Cisco IOS Software Image, page 3-47
- Booting from the Cisco IOS Software Image, page 3-48

PRP Interfaces Using the PRP LEDs

The PRP faceplate has eight device or port LED activity indicators. (See Figure 3-24.) Each LED goes on when its corresponding PCMCIA slot is accessed. The ports are as follows:

- Two PCMCIA slot activity LEDs labeled SLOT-0 and SLOT-1.
- Four RJ-45 Ethernet port activity LEDs. These LEDs are used by the RJ-45 Ethernet connectors. Each connector includes four LEDs that indicate link activity (LINK), port enabled (EN), data transmission (TX), and data reception (RX).
- Two Ethernet port-selection LEDs labeled PRIMARY. These two LEDs, when on, identify which of the two Ethernet connections is selected. Because both ports are supported on the PRP, the LED on port ETH0 is always on. The ETH1 LED goes on when it is selected.

Figure 3-24 PRP LEDs



LINK	Indicates link activity
EN	Indicates the port is enabled
TX	Indicates data transmission
RX	Indicates data reception

When you start an unconfigured system for the first time, the console screen displays a system banner and then automatically starts the System Configuration Dialogue. Observe the Cisco IOS banner on the console screen. If a Flash memory card containing a valid Cisco IOS software image is inserted in PCMCIA slot 0 and the software configuration register is set to 0x0102 (the factory default setting), the router automatically boots using this image.

As the router boots the Cisco IOS software image, the console screen displays a system banner similar to the following:

```
Cisco Internetwork Operating System Software
IOS (tm) GS Software (GSR-P-M)
12.0(20020120:204554)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Sat 20-Aug-01 18:34
.
.
.
```

Note The system banner that you see depends on the image version of the Cisco IOS software that the system is running.

If the ROM monitor prompt (`rommon>`) appears on the system console, your router did not find a valid system image, or the boot sequence was otherwise interrupted, and the system entered read-only memory (ROM) monitor mode.

To boot a Cisco IOS software image manually, enter the **boot** command on the system console. For information on using the various forms of the **boot** command, see the following sections:

- Locating a Valid Cisco IOS Software Image, page 3-47
- Booting from the Cisco IOS Software Image, page 3-48

System Configuration Dialogue

The following information is an example of a System Configuration Dialog interactive script message that appears on the system console. This interactive script prompts you through the steps to create a router configuration database file defining basic system operation parameters.

```
         --- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]:
```

External Network Interface

After configuration, the RP and line cards can communicate with external networks. You do not need to configure the network interfaces immediately, but you cannot connect to a network until you configure the interfaces for operation in your networking environment. For configuration information, see the "Router Configuration" section on page 3-49.

Note The interface-specific LEDs on the line cards go on when the line card interfaces are configured.

To verify correct operation of each line card interface, complete the first-time setup procedures and configuration, then check the status of the interfaces against the LED descriptions in the configuration notes for each line card.

If the system does not complete each of the boot process steps, see Chapter 4, "Troubleshooting the Installation."

Manually Booting the System

If your router does not find a valid system configuration image, or if you interrupt the boot sequence, the system might enter read-only memory (ROM) monitor mode and display the ROM monitor prompt (`rommon>`). From ROM monitor mode, you have access to a number of commands to locate and boot a valid system image.

Locating a Valid Cisco IOS Software Image

To locate a Cisco IOS software image for manually booting the router from the ROM monitor prompt (`rommon>`), follow the steps below:

Step 1 Use the ROM monitor mode **dir bootflash** command to examine the contents of the onboard Flash memory SIMM (NVRAM) on the RP:

```
rommon 1> dir bootflash:
   File size                   Checksum      File name
   3277967 bytes (0x32048f)   0x6b331e30    gsr-p-mz.120-7.4.5
rommon 2>
```

Step 2 If the onboard Flash memory SIMM contains the desired Cisco IOS boot image, proceed to the "Booting from the Cisco IOS Software Image" section on page 3-48. Otherwise, continue looking for a valid image by examining the contents of the Flash memory card in either PCMCIA slot 0 or slot 1 on the RP.

You can determine the content of the card by issuing the ROM monitor mode **dir slot*n*:** command, where *n* represents either 0 (slot 0) or 1 (slot 1). The following example of the command lists the contents of the Flash memory card in slot 0:

```
rommon 2> dir slot0:
   File size                   Checksum      File name
   3277967 bytes (0x32048f)   0x6b331e30    gsr-p-mz.120-7.4.5
rommon 3>
```

Booting from the Cisco IOS Software Image

After locating a valid Cisco IOS software image, you can boot from that image manually by issuing the appropriate ROM monitor mode **boot** commands from the list in Table 3-13.

Table 3-13 ROM Monitor Boot Commands

Command	Description
boot	(No argument.) Boots the default image found in the onboard Flash memory SIMM. The image is loaded into the SIMM at the factory.
boot flash	Attempts to boot the router using the first file found in the Flash memory card inserted in slot 0 of the RP.
boot slot0: *filename*	Boots the router using the specified file from the Flash memory card in slot 0 of the RP.
boot slot1: *filename*	Boots the router using the specified file from the Flash memory card in slot 1 of the RP.
boot bootflash: *filename*	Boots the router using the specified file from the onboard Flash memory SIMM (NVRAM) on the RP.
boot tftp: *filename* [*host*]	Boots the router using the specified file from a host TFTP server in the network.

Ensure that the Flash memory card inserted in PCMCIA slot 0 contains a valid Cisco IOS software image. Otherwise, the system will boot an invalid image from the Flash memory card. To examine the contents of a Flash memory card, enter the **dir slot***n***:** command.

If you did not change the contents of the software configuration register, the factory default setting of 0x0102 in the software configuration register causes the system to boot Cisco IOS software from a Flash memory card inserted in PCMCIA slot 0 the next time you boot the router.

Router Configuration

You can perform a basic configuration for your router by using either the **setup** command automatic prompt method, or the global configuration method in which you enter each option and parameter manually. Configuration is described in these sections:

- Before You Begin, page 3-49
- setup Command, page 3-49
- Global Configuration Mode, page 3-50

Before You Begin

Before you begin the configuration process for your router, you should have the following information available:

- Interfaces the router will use
- Routing protocols the router will support
- Network addresses for the protocols being configured
- Password scheme for your environment

setup Command

One option is to use the **setup** command, also known as the **setup** command utility. During the first startup of an unconfigured router, the system automatically starts the **setup** command utility, which enables you to begin configuring your router. The **setup** command utility presents a structured, interactive script that guides you through the process.

You can invoke the **setup** command utility at any time by issuing the **setup** command at the privileged EXEC mode prompt (`Router#`), which invokes the same configuration script that appears automatically during the first startup of an unconfigured router. You can enter the **setup** command at any time to alter previously entered configuration information.

The advantage in using the **setup** command utility is that the system uses an interactive script to guide you through the configuration process.

Global Configuration Mode

The router can be configured manually using the global configuration mode through the Cisco IOS command line interface (CLI). This method requires you to enter configuration commands on a line-by-line basis at the system console, without being prompted by the **setup** command configuration script.

Cisco IOS User Interface

The Cisco IOS software provides a command line interface by which you can configure and manage your router. If you are unfamiliar with the Cisco IOS command line interface, refer to the "Using the Command Line Interface" chapter in the Cisco *Configuration Fundamentals Configuration Guide*, which discusses different command modes, context-sensitive help, and editing features.

User Interface Command Modes

The Cisco IOS user interface is organized into many different modes. The commands that are available depend on which mode you are currently in. Entering a question mark (?) at the system prompt displays a list of commands available for the current command mode.

When you start a session on the router, you begin in user mode, often called EXEC mode. Only a limited subset of commands are available in EXEC mode. To have access to all commands, enter privileged EXEC mode, which requires that you enter a password. From privileged EXEC mode, you can enter any EXEC command or enter global configuration mode. Most of the EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The EXEC commands are not saved across reboots of the router.

The configuration modes allow you to make changes to the running configuration. If you later save the configuration, these commands are stored and can be used when you reboot your router. Starting at global configuration mode, you can enter interface configuration mode, subinterface configuration mode, and other protocol-specific modes.

ROM monitor mode is a separate mode used when the router cannot boot properly. If the router does not find a valid system image when it is booting, or if the router configuration file is corrupt at startup, the system might enter ROM monitor mode.

User EXEC Mode

After the router boots successfully and loads the Cisco IOS software, the system software displays the user EXEC mode prompt on the system console. The user EXEC mode prompt consists of the assigned router host name plus the greater than bracket (>). The default host name is `router` unless it has been changed during initial configuration using the **setup** command facility. The user EXEC mode prompt for a router with the factory default name is Router.

```
Router>
```

Privileged EXEC Mode

Because many of the privileged commands set operating parameters, privileged access should be password protected to prevent unauthorized use. To enter privileged EXEC mode, enter the **enable** command at the user EXEC mode prompt. If the **enable** secret password was set and saved in memory, the system prompts you to enter the **enable** secret password. The password is not displayed on the screen and is case sensitive. When the system accepts the password, it changes the prompt to the privileged EXEC mode prompt, which consists of the assigned router host name followed by the pound sign (#). The following example shows the change from user EXEC mode to privileged EXEC mode on the router named Router.

```
Router> enable
password: <password>
Router#
```

For information about using passwords, see the "Configuring Global Parameters" section on page 3-57.

Global Configuration Mode

Global configuration commands apply to features that affect the system as a whole, rather than just one protocol or interface. Use the **configure terminal** privileged EXEC command to enter global configuration mode. Commands to enable a particular routing or bridging function are global configuration commands.

Interface Configuration Mode

Many features are enabled on a per-interface basis. Interface configuration commands modify the operation of an interface, such as Ethernet, FDDI, or serial port. Interface configuration commands always follow an **interface** global configuration command, which defines the interface type.

For details on interface configuration commands that affect general interface parameters, such as bandwidth or clock rate, refer to the "Interface Commands" chapter in the *Configuration Fundamentals Command Reference*. For protocol-specific commands, see the appropriate Cisco IOS software command reference.

Subinterface Configuration Mode

You can configure multiple virtual interfaces (called subinterfaces) on a single physical interface. Subinterfaces appear to be distinct physical interfaces to the various protocols. For detailed information on how to configure subinterfaces, see the appropriate module for a specific protocol in the Cisco IOS software documentation.

ROM Monitor Mode

If your router does not find a valid system image, or if you interrupt the boot sequence, the system might enter read-only memory (ROM) monitor mode. From ROM monitor mode, you can boot the system or perform diagnostic tests. You also can enter ROM monitor mode by entering the **reload** EXEC command and then pressing the Break key during the first 60 seconds of startup.

Configuration Changes

This section describes how to configure the router. It includes information on the following topics:

During the first-time startup of an unconfigured router, the system automatically starts the **setup** command utility and begins displaying the interactive System Configuration Dialog on the system console screen. The System Configuration Dialog guides you through the configuration process with prompts for global (system-wide) parameters and interface (line card) parameters.

The System Configuration Dialog prompts and the order in which they appear on the screen vary depending on the platform, interfaces installed, router, and the Cisco IOS software image the router is running.

Let the entire System Configuration Dialogue script run, until you come to the item that you want to change. To accept default settings for items that you do not want to change, press the console keyboard **Return** key. To return to the privileged EXEC prompt without making changes, press **Ctrl-C**. To access help text in the setup command utility, press the question mark key (?) at any prompt.

When you complete your changes, the **setup** command utility displays the configuration command script that was created as a result of the changes entered during the setup session. It also queries if you want to use this configuration. If you answer Yes, the configuration is saved to NVRAM. If you answer No, the configuration is not saved and the process begins again. There is no default for this prompt; you must answer either Yes or No.

The "setup Command Interactive Script Example" section on page 3-54, shows a setup session automatically invoked during the first-time startup of the router. During first-time startup, the system displays the system banner information, then starts the System Configuration Dialog.

The output shown in this example depends on the image version of the Cisco IOS software and the way your router is equipped. Your configuration dialog might be different.

The **setup** command script is a self-guiding interactive script that prompts you for responses and provides default or alternative values wherever possible.

setup Command Interactive Script Example

```
Cisco Internetwork Operating System Software
.
.
.
         --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: Yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic setup only configures enough connectivity
for management of the system, extended setup will ask you
to configure each interface of the system.

Would you like to enter basic management setup? [yes/no]: Yes
Configuring global parameters:

  Enter host name [Router]: Router

  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret [<Use current secret>]: alpha

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: bravo

  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: charlie
  Configure SNMP Network Management? [no]:
```

```
Current interface summary
Interface    IP-Address      OK? Method Status                Protocol
Ethernet0    unassigned      YES unset  administratively down down
POS1/0       unassigned      YES unset  administratively down down
SDCC1/0      unassigned      YES unset  administratively down down
POS2/0       unassigned      YES unset  administratively down down
SDCC1/0      unassigned      YES unset  administratively down down
.
.
.
POS15/0      unassigned      YES unset  administratively down down
SDCC15/0     unassigned      YES unset  administratively down down

Enter interface name used to connect to the
management network from the above interface summary: Ethernet0

Configuring interface Ethernet0:
Configure IP on this interface? Yes
  IP address for this interface: 172.99.99.2
  Subnet mask for this interface: 255.85.89.000
Class B network is 172.88.9.0, 8 subnet bits; mask is /24

The following configuration command script was created:

hostname Router
enable secret 5 $1$krIg$emfYm/1OwHVspDuS8Gy0K1
enable password wilma
line vty 0 4
password charlie
no snmp server
!
no ip routing
!
interface Ethernet0
no shutdown
ip address 172.88.99.2 255.888.255.0
!
interface POS1/0
shutdown
no ip address
!
interface SDCC1/0
shutdown
no ip address
.
.
.
```

```
interface POS15/0
shutdown
no ip address
!
interface SDCC15/0
shutdown
no ip address
!
end
[0] Go to the IOS command prompt without saving this script.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]:

Building configuration ...

Use the enabled mode ‘configure’ command to modify this configuration.

router#
```

You can enter the **setup** command at any time at the privileged EXEC prompt to activate the **setup** command utility.

The only observable difference between the configuration script displayed when the **setup** command utility starts automatically on startup, and the script displayed when you enter the **setup** command, is that the existing script displays any previously entered system configuration defaults within square brackets ([ ]).

For example, during the configuration of a POS interface that has not been previously configured, when using the **setup** command utility at startup, you will see a display in the following form as you proceed through the script and respond to the prompts:

```
Configuring interface POS1/0:
  Is this interface in use?: yes
  Configure IP on this interface?: yes
```

In this example, the script does not display default or current conditions in square brackets ([ ]), because the **setup** command utility ran automatically at startup and there was no prior configuration information.

When you enter the **setup** command at the privileged EXEC mode prompt, assuming that the POS interface *has been* configured previously and you are being queried by the system for changes, you will see a display in the following form:

```
Configuring interface POS1/0:
  Is this interface in use?[yes]:
```

```
Configure IP on this interface?[yes]:
```

The script displays the default or current conditions of the interface in square brackets, ([ ]) because you invoked the **setup** command utility using the **setup** command and there is previous configuration information. When a system prompt contains an existing default value in square brackets, press **Return** to accept the default value, or type an alternate value and press **Return**.

Configuring Global Parameters

When you first enter the **setup** utility or invoke the **setup** command, the system prompts you to configure global parameters for your router. The global parameters are used for controlling system-wide settings, including the following:

- Host name for the router
- Passwords for the enable secret, enable, and virtual terminal security parameters
- Protocols used by the router

Host Name

The name you assign the router must follow the rules for ARPANET host names. It must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. The name must consist of 63 or fewer characters. For more information, refer to *Requests For Comments (RFC) 1035, Domain Names—Implementation and Specifications*.

Upper- and lowercase characters look the same to many Internet software applications; therefore, computer names should appear in all lowercase. For more information, refer to *RFC 1178, Choosing a Name for Your Computer.*

Passwords

The commands available at the user EXEC level are a subset of those available at the privileged EXEC level. Many privileged EXEC commands are used to set system parameters. You should password-protect these commands to prevent their unauthorized use. For information on how to establish password protection or configure privilege levels, refer to the “Configuring Passwords and Privileges”

chapter in the *Security Configuration Guide*. This document is part of the Cisco IOS software configuration documentation set that corresponds to the Cisco IOS software release installed on your Cisco hardware.

The ***enable secret*** password functionality is available for Cisco 12006 and Cisco 12406 Routers. You must enter the correct password on the system console to gain access to privileged-level commands. When you are running from the ROM monitor, you can use the ***enable*** password, depending on your boot ROM level.

For maximum security, the **enable secret** and the **enable** passwords should be different. If you use the same password for both functions during the **setup** process, the system accepts it but warns that you should enter a different password.

An **enable secret** password can contain from 1 to 25 uppercase and lowercase alphanumeric characters; an **enable** password can contain any number of uppercase and lowercase alphanumeric characters. A number cannot be used as the first character. Spaces, however, are valid password characters. For example, `two words` is a valid password. Leading spaces are ignored, but trailing spaces are recognized. Make a note of all passwords you set, and store that information in a secure location for future reference.

Protocols

For complete information on protocol configuration for your router, refer to the appropriate software configuration publications, which are listed in the "If You Need More Information" section on page 3-82.

Configuring Network Interfaces

This section summarizes information about configuring the network interfaces for the RP and the installed line cards by using the **setup** command utility or **setup** command. Once configured, the RP and line cards can communicate with external networks.

To configure the interface parameters for the RP and installed line cards, you need the following information:

- Interface network addresses
- Subnet mask values

- Protocols to be configured

To obtain this information, consult your network administrator. For additional interface configuration information for the RP and each of the line cards installed in your router, refer to the configuration note that shipped with each card.

GRP Ethernet Interfaces

The RJ-45 and MII receptacles on the faceplate of the GRP are IEEE 802.3u-compliant interfaces. These IEEE interfaces provide connectivity to Ethernet networks. You can use either interface, but not both at the same time.

The following configuration dialog example shows the system being configured for an Ethernet interface that will use the IP network layer protocol. (The Ethernet interface does not support external routing functions.) The IP address and subnet mask value below are examples. The actual IP address and subnet mask value would be different.

```
Configuring interface Ethernet0:
  Is this interface in use?: yes
  Configure IP on this interface?: yes
    IP address for this interface: 3.3.1.1
    Number of bits in subnet field: 8
    Class A network is 3.0.0.0, 8 subnet bits; mask is 255.888.0.0
  Configure CLNS on this interface?: yes
```

PRP Ethernet Interfaces

The IEEE 802.3 Ethernet interfaces on the PRP allow connections to external Ethernet networks and can transmit data rates of 10 Mbps and 100 Mbps. The transmission speed of the Ethernet ports is auto-sensing by default and is user configurable.

Caution The Ethernet ports are primarily used as Telnet ports into the router, or for booting or accessing Cisco IOS software images over a network to which an Ethernet port is directly connected. Cisco Express Forwarding (CEF) functions are switched off by default for security reasons. Cisco strongly cautions you to consider the security implications of switching on CEF routing functions on these ports.

Line Card Interfaces

Because of the wide variety of line cards supported by Cisco 12006 and Cisco 12406 Routers, you should see the configuration note that shipped with a particular card for interface configuration information. This section provides several examples to show the general way the **setup** command utility handles line card interface configuration.

The following sample excerpt from a System Configuration Dialog session for a Quad OC-3cPOS line card shows settings for a typical configuration:

```
Configuring interface POS3/0:
  Is this interface in use?: yes
  Configure IP on this interface?: yes
  Configure IP unnumbered on this interface?: no
    IP address for this interface: 2.1.1.1
    Number of bits in subnet field: 0
    Class A network is 2.0.0.0, 0 subnet bits; mask is 255.9.0
  Configure CLNS on this interface?: yes
```

Note By default, POS interfaces use the 32-bit cyclic redundancy check (CRC) and high-level data link control (HDLC) as the encapsulation protocol.

The following sample shows the same Quad OC-3c POS line card interface being configured for IP unnumbered:

```
Configuring interface POS3/0:
  Is this interface in use?: yes
  Configure IP on this interface?: yes
  Configure IP unnumbered on this interface?: yes
    Assign to which interface: ethernet0
  Configure CLNS on this interface?: yes
```

In the following sample, an ATM line card is being configured to use IP:

```
Configuring interface parameters:

Configuring interface ATM1/0:
  Is this interface in use?: yes
  Configure IP on this interface?: yes
    IP address for this interface: 1.1.1.2
    Number of bits in subnet field: 0
    Class A network is 1.0.0.0, 0 subnet bits; mask is 255.9.8.0
```

Note You might have to establish additional configuration parameters for the installed ATM line cards if you want to use all their capabilities. For example, additional steps are required to configure permanent virtual circuits (PVCs).

After you have manually configured the network interface parameters using the **setup** command utility or the **setup** command, your RP and line card interfaces are available for limited use. To modify the currently saved configuration information, enter the **setup** command at the privileged EXEC mode prompt (`Router#`) at any time to start another System Configuration Dialog session.

To perform more complex configuration tasks, enter the **configure terminal** command at the privileged EXEC mode prompt (`Router#`) to invoke the global configuration mode [`Router(config)#`].

Checking the Software Version

To determine the current version of the Cisco IOS software running on your router, enter the **show version** command at the user EXEC prompt. The Cisco IOS software version number is displayed, as well as other information, including the hardware installed in the system, the names and sources of system image files, and the contents of the software configuration register. The **show version** command also identifies the type of router.

The example in the show version Command section that follows below shows typical results from the **show version** command. Depending on the image version of the Cisco IOS software running on your router and the way it is equipped, the results of your **show version** command might be different.

show version Command

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) GS Software (GSR-P-M)
12.0(20020120:204554)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Sat 20-Aug-01 18:34
Image text-base: 0x60010950, data-base: 0x61C00000

ROM: System Bootstrap, Version 11.2(17)GS2, [name 180] EARLY
DEPLOYMENT RELEA)
```

```
BOOTFLASH: GS Software (GSR-BOOT-M), Version 11.2(18)GS4, EARLY
DEPLOYMENT RELE

Getty uptime is 22 hours, 15 minutes
System returned to ROM by reload
System image file is "tftp://xxx.xx.xx.xxx/directory/name/gsr-p-mz"

cisco 12406/GRP (R5000) processor (revision 0x05) with 262144K bytes
of memory.
R5000 CPU at 200Mhz, Implementation 35, Rev 2.1, 512KB L2 Cache
Last reset from power-on

1 Route Processor Card
.
.
.
Configuration register is 0x0
.
.
.

router#
```

Verifying the Running Configuration Settings

To check the running configuration settings or any changes made to settings before you save them, enter the **show running-config** command at the privileged EXEC mode prompt. For a Quad OC-3c/STM-1c POS interface installed in slot 1, the **show running-config** command typically displays output in the form shown in the example below. Depending on the image version of the Cisco IOS software running on your router and the way it is equipped, the results of your **show running-config** command might be different.

show running Config Command Example

```
router# show running-config
Building configuration...

Current configuration:
!
version 12.0
no service pad
no service udp-small-servers
```

```
no service tcp-small-servers
!
hostname Router
!
enable secret 5 $1$W6K5$W/p5Bq6IPLGJ/hS9VVP1g.
enable password twink

interface POS1/0
 ip address 10.1.1.1 255.888.255.0
 crc 32
 clock source internal
!
interface POS1/1
 no ip address
 no ip route-cache cef
 no ip route-cache
 shutdown
 crc 32
!
interface POS1/2
 no ip address
 no ip route-cache cef
 no ip route-cache
 shutdown
 crc 32
!
interface POS1/3
 no ip address
 no ip route-cache cef
 no ip route-cache
 shutdown
 crc 32
```

Note For more information on a specific line card, see the line card installation and configuration note that came with your line cards.

You can access Cisco IOS software documentation and hardware installation and maintenance documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

Saving the Running Configuration Settings to NVRAM

To save the running configuration changes to NVRAM, enter the **copy running-config startup-config** command at the privileged EXEC mode prompt as follows:

```
Router# copy running-config startup-config
```

You can also use the following command to save the running configuration settings:

```
Router# write memory
```

Either command saves to NVRAM the configuration settings that you created while in the global configuration mode. If you do not save the running configuration settings to NVRAM, your configuration settings will be lost the next time you reload the system.

Reviewing the Running Configuration Settings

To display the running configuration settings stored in NVRAM, enter the **show startup-config** command at the privileged EXEC mode prompt on the system console. This command displays output in the form shown in the example that follows below. Depending on the image version of the Cisco IOS software running on your router and the way it is equipped, the results of your **show startup-config** command might be different.

show startup-config Command

```
Router# show startup-config
Using 5560 out of 520184 bytes
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
enable secret 5 $1$/5HX$OOvyhG2JYhNaCbPa45Wmn/
enable password wilma
```

```
ip cef distributed switch
ip host biff 10.3.3.254
!
interface Ethernet0
 ip address 10.3.1.1 255.888.0.0
 no ip mroute-cache
!
interface POS1/0
 ip address 10.1.1.1 255.8.9.0
 no keepalive
 crc 16
 no cdp enable
.
.
.
interface ATM3/0
 ip address 10.0.0.15 255.8.8.0 secondary
 ip address 10.1.1.2 255.8.8.0
 atm pvc 1 0 64 aal5snap
 atm pvc 2 0 72 aal5mux ip 155000 155000 1
 atm pvc 3 1 90 aal5snap 312000 312000 1
 atm pvc 4 0 108 aal5snap
 atm pvc 10 0 144 aal5mux ip 155000 155000 1
 atm pvc 11 1 91 aal5snap 310000 310000 1
 map-group atm1
!
no ip classless
ip route 10.5.8.254 255.888.255.255 Ethernet0
!
map-list atm1
 ip 10.1.1.1 atm-vc 1
 ip 10.1.1.3 atm-vc 2
 ip 10.1.1.4 atm-vc 4
 ip 10.0.0.1 atm-vc 3
 ip 10.0.0.5 atm-vc 10
 ip 10.0.0.6 atm-vc 11
no logging trap
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password bambam
 login
!
end
Router#
```

Using Flash Memory Cards in the RP

This section describes how to use Flash memory cards in the RP and includes information on the following topics:

Installing the Flash Memory Card in a RP

If there are dual RPs, the PCMCIA slots in the primary RP are designated slot 0 and slot 1. If there is a second RP, the PCMCIA slots in the second RP are designated sec-slot 0 and sec-slot 1. PCMCIA slot 0 is the bottom slot and slot 1 is the top slot. Both Flash memory card slots on each RP can be used at the same time. The following generic procedure can be used to install a Flash memory card in either slot position.

Step 1 Facing the RP faceplate, hold the Flash memory card with the connector end of the card toward the slot and the label facing up. (See Figure 3-10 on page 3-21.)

Step 2 Insert the card into the appropriate slot until the card completely seats in the connector at the back of the slot and the ejector button pops out toward you.

Removing the Flash Memory Card from an RP

To remove a Flash memory card, follow these steps:

Step 1 Press the appropriate ejector button until the card is free of the connector at the back of the slot.

Step 2 Pull the card from the slot and place it in an antistatic sack to protect it from ESD damage.

The Flash memory card is keyed for proper insertion. The ejector button will not pop out unless the card is inserted correctly. Part of the card remains outside the slot even when the card is properly seated. Do not attempt to force the card deeper into the slot after the ejector button pops out.

Formatting a Flash Memory Card

The Flash memory card that shipped with your router contains the default Cisco IOS software image you need to boot your router.

Warning **This procedure erases all information on a Flash memory card. To prevent the loss of important data that might be stored on a Flash memory card, proceed carefully.**

If you want to save the data on a Flash memory card, copy the data to a server before you format the card. In some cases, you might need to insert a new Flash memory card and copy images or backup configuration files to the card. Before you can use a new Flash memory card, you must format it. Use only Type I or Type II Flash memory cards.

Caution The following formatting procedure presumes you have already booted your router.

To format a new Flash memory card, follow these steps:

Step 1 Insert the Flash memory card into slot 0 or slot 1 on the RP. (This example uses slot 0.)

Step 2 Enter the **format slot0:** command at the privileged EXEC mode prompt on the system console:

```
Router# format slot0:
All sectors will be erased, proceed? [confirm]
Enter volume id (up to 30 characters): MyNewCard
Formatting sector n
Format device slot0 completed
Router#
```

The console displays the "Formatting sector *n*" line in the sample output shown above. When the count reaches 1, the formatting process is complete and the new Flash memory card is ready for use.

For complete command descriptions and configuration information, refer to the *Configuration Fundamentals Command Reference* and the *Configuration Fundamentals Configuration Guide* in the Cisco IOS documentation set. For information on obtaining these publications, see the "If You Need More Information" section on page 3-82.

Specify a Boot Image

Use the procedure in this section to identify a sample Cisco IOS software image (*new.image* in this example) that is to be made bootable from a Flash memory card. The software configuration register must be set to 0x2102 during this procedure to boot the image from a Flash memory card; therefore, the **config-register** command must be included in the command sequence, as shown in this example:

```
Router# configure terminal
Router(config)# no boot system
Router(config)# boot system flash slot0:new.image
Router(config)# config-register 0x2102
Ctrl-Z
Router# copy running-config startup-config
Router# reload
```

When you enter the **reload** command, the specified file (*new.image*) on the Flash memory card inserted in PCMCIA slot 0 is used to boot the system.

If one of the following software configuration register settings were specified in the preceding example, the system would behave accordingly:

- 0x2000—If the network boot fails, the system boots a default Cisco IOS software image from a Flash memory card.
- 0x0100—The system ignores the Break function.
- 0x0101—The system boots the default image (the first image found) from the onboard Flash memory SIMM on the RP. This setting also tells the system that it should *not* reset the Break disable function, nor should it check for a default filename for booting over the network.
- 0x0002—The system looks in the Flash memory SIMM on the RP for a default Cisco IOS software image.
- 0x0102—The system disables the Break function and checks for a default TFTP server filename. If the network boot operation fails, the system boots from a Flash memory card.

Flash Memory Console Commands

To determine whether the present working device you are accessing is the onboard Flash SIMM on the RP or a PCMCIA Flash memory card in a slot on the RP, enter the **pwd** command at the privileged EXEC mode prompt on the system console as follows:

```
Router# pwd
slot0:
Router#
```

In this example, the present working device you are accessing is on a PCMCIA Flash memory card inserted in slot 0 of the RP.

To change from one type of Flash memory device access to another, enter the **cd** *device-name* command, where *device-name* can be **slot0:**, **slot1:**, or **bootflash:**.

Sample uses of the **cd** command include:

```
Router# cd slot1:
Router# pwd
```

```
slot1:/
Router# cd slot0:
Router# pwd
slot0:/
Router# cd bootflash:
Router# pwd
bootflash:/
Router#
```

To list the directory contents of the Flash memory media in use, enter the **dir** [*device-name*] command at the privileged EXEC mode prompt, where *device-name* can be **slot0:**, **slot1:**, or **bootflash:**.

A sample use of the **dir** command follows.

```
Router# dir
Directory of slot0:/

  1  -rw-     122015   Sep 30 2002 15:03:55 myfile1
  2  -rw-    2054979   Sep 30 2002 15:17:33 gsr-diag-mz.RELEASE28
  3  -rw-    6670560   Sep 30 2002 15:22:49 gsr-p-mz.p7
  4  -rw-       5560   Oct 08 2002 16:54:53 info

20578304 bytes total (9661756 bytes free)
Router#
```

To delete a file from a Flash memory media, use the **cd** command to select the Flash memory media and enter the **delete** *filename* command at the privileged EXEC mode prompt, where *filename* is any file within the selected Flash memory media.

An example of deleting the file *info* from the current Flash memory directory follows:

```
Router# delete slot0:info
Router# dir
Directory of slot0:/

  1  -rw-     122015   Sep 30 2002 15:03:55 myfile1
  2  -rw-    2054979   Sep 30 2002 15:17:33 gsr-diag-mz.RELEASE28
  3  -rw-    6670560   Sep 30 2002 15:22:49 gsr-p-mz.p7

20578304 bytes total (9661756 bytes free)
Router#
```

Files that are deleted from the current Flash memory directory are removed from the directory list, but are not erased; they still occupy space in Flash memory. This feature allows you to recover a deleted file later using the **undelete** command.

To remove deleted files from a Flash memory directory permanently, but leave undeleted files intact, enter the **squeeze** *device-name* command at the privileged EXEC mode prompt on the system console, where *device-name* can be **slot0:**, **slot1:**, or **bootflash:**. The **squeeze** command permanently removes deleted files and makes all other undeleted files contiguous, thus conserving storage space.

To prevent loss of data due to sudden power loss, the squeezed data is temporarily saved to another Flash memory area reserved specifically for system use.

An example of the **squeeze** command follows.

```
Router# squeeze slot0:
All deleted files will be removed, Continue? [confirm]y
Squeeze operation may take a while, Continue? [confirm]y
Squeeze of slot0 complete
Router#
ebESZ
```

In the preceding example command display, the characters in the final line (ebESZ) represent the Flash memory operations performed during the execution of the **squeeze** command. Table 3-14 describes these indicators.

Table 3-14 Squeeze Command Functions Example

e	The special Flash memory area has been erased. This erase operation must be accomplished before any write operation to the special Flash memory area can begin.
b	The data about to be written to the special Flash memory area has been temporarily copied.
E	The sector temporarily occupied by the data has been erased.
S	The data has been written to its permanent location in Flash memory.
Z	The log has been erased following the successful **squeeze** operation.

During the squeeze operation, the system maintains a log identifying which of the squeeze functions has been accomplished, so that the system can return to the proper place and continue the operation in the event of a power failure.

Booting from Flash Memory

To enable booting from Flash memory, set the boot field in the software configuration register (bits 3 through 0) to a value between 2 and 15. These values are used with the **boot system flash** *device:filename* configuration command, where *device* is **bootflash:**, **slot0:**, or **slot1:**, and *filename* is the name of the file from which you want to boot the system.

To enter global configuration mode while the system is running and specify a Flash filename from which to boot the system, enter the **configure terminal** command at the privileged EXEC mode prompt on the system console, as follows:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# boot system flash device:filename
```

To disable the Break function and enable the **boot system flash** *device*:*filename* command, enter the **config-register** command at the global configuration mode prompt with the configuration register value, as shown below:

```
Router(config)# config-reg 0x0102
Ctrl-Z
Router#
```

Copying Files

Copy a new Cisco IOS software image to Flash memory when a new image becomes available or when you want to back up the image. This section explains how to copy any type of file to the Flash memory SIMM on the RP or to a PCMCIA Flash memory card inserted in either slot 0 or slot 1.

Caution You cannot copy a new Cisco IOS software image into the onboard Flash memory SIMM (also referred to as bootflash) while the system is running from onboard Flash memory.

To avoid losing valid Cisco IOS images, upgrade your Cisco IOS software images in Flash memory one at a time. Upgrade your PCMCIA-based Flash memory separately from the onboard Flash SIMM (bootflash) on the RP.

To copy a file to Flash memory, enter the following command at the privileged EXEC mode prompt on your system console:

Router# copy tftp:*filename* [**bootflash:**|**slot0:**|**slot1:**] *filename*

where:

tftp:*filename*	Specifies the source and name of the file to be copied.
[**bootflash:** | **slot0:** | **slot1:**] *filename*	Specifies the destination Flash medium and name for the new file. The destination Flash medium can be one of the following: **bootflash:**—The file will be copied to the onboard Flash memory SIMM on the RP. **slot0:**—The file will be copied to the PCMCIA Flash memory card in slot 0. **slot1:**—The file will be copied to the PCMCIA Flash memory card in slot 1.

Example of output generated by a **copy tftp:***filename* command:

```
Router# copy tftp:myfile1 slot0:myfile1
20575008 bytes available on device slot0, proceed? [confirm]
Address or name of remote host [1.1.1.1]?
Loading new.image from 1.1.1.1 (via Ethernet0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!![OK - 7799951/15599616 bytes]
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
Router#
```

In this example, the exclamation points `(!)` appear as the source file is being downloaded to the destination device. The `ccccc` characters indicate that a cyclic redundancy check (CRC) is being calculated during the downloading process. The CRC verifies that the file has been correctly downloaded to the Flash memory card inserted in PCMCIA slot 0 or the designated destination device.

Copying a Cisco IOS Software Image

You can copy a Cisco IOS software image into a Flash memory card at any time for later use, but you must first format the Flash memory card that you will use in the copy operation. If you have not already formatted the card, see the "Formatting a Flash Memory Card" section on page 3-67.

To ensure access to the network TFTP server, you must configure one network interface using the **setup** command facility. For instructions on using this facility, see the "Configuration Changes" section on page 3-53 or refer to the *Configuration Fundamentals Configuration Guide* for the IOS software release running on this router.

To copy a bootable image into the Flash memory card, follow these steps:

Step 1 Boot the router and allow it to initialize.

Step 2 Enter the **enable** command at the user EXEC mode prompt to enter privileged EXEC mode:

```
Router> enable
Password: <password>
Router#
```

Step 3 Copy the file named *new.image* in this example to the Flash memory card inserted in PCMCIA slot 0 by using the following command:

```
Router# copy tftp:new.image slot0:new.image
20575008 bytes available on device slot0, proceed? [confirm]
Address or name of remote host [1.1.1.1]?
Loading new.image from 1.1.1.1 (via Ethernet0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 7799951/15599616 bytes]
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCC
Router#
```

In this example, the exclamation points `(!)` appear as the source file is being downloaded to the destination device. The `CCCCC` characters indicate that a cyclic redundancy check (CRC) is being calculated during the downloading process. The CRC verifies that the file has been correctly downloaded to the Flash memory card inserted in PCMCIA slot 0 or the designated destination device.

Step 4 Reboot the system.

Copying Cisco IOS Software Updates

As future releases of Cisco IOS software become available, you will receive these images as a file booted from a network TFTP server, as a file on a floppy disk, or as a file on a Flash memory card.

This section explains how to use a newly released Cisco IOS software image on a Flash memory card in a system that has an older Cisco IOS image residing on a Flash memory card inserted in PCMCIA slot 0 and a default Cisco IOS software boot image stored in the onboard Flash memory SIMM on the RP.

In this procedure, you will copy an updated Cisco IOS software image from a new Flash memory card onto a Flash memory card containing an old Cisco IOS software image. In this example, the following filenames apply:

- *image.new*—The new image on the new Flash memory.
- *image.old*—The old image on the old Flash memory card inserted in PCMCIA slot 0.
- *image.boot*—The bootable Cisco IOS software image stored in the onboard Flash memory SIMM. (This image is used by default to boot the system if no other bootable image is available.)

This procedure assumes that there is sufficient space on the old Flash memory card inserted in slot 0 for both the new Cisco IOS software image and the old image. If there is not enough space for both images on the old Flash memory card, use the **delete** command to delete files from the old Flash memory card, but *do not* delete the *image.old* file. After deleting files, use the **squeeze** command to remove the deleted files from the old Flash memory card permanently. For information on the **squeeze** command, see the "Flash Memory Console Commands" section on page 3-69.

If the two files still will not fit on the Flash memory card in slot 0 after you delete files and use the **squeeze** command, remove this card, place it in an antistatic bag for ESD protection, and store it in a safe place. Insert the Flash memory card containing *image.new* in slot 0. Proceed to Step 5 in the following procedure and enter the command **boot system flash slot0:image.new** to designate the file *image.new* as the new default Cisco IOS software boot image.

To copy a bootable Cisco IOS software image between Flash memory cards, follow these steps:

Step 1 Boot the router. For this example, the file named *image.boot* is the default boot image.

Step 2 Enter the **enable** command to enter privileged EXEC mode as follows:

```
Router> enable
Password: <password>
Router#
```

Step 3 Insert the new Flash memory card in slot 1.

Step 4 Enter the following command to copy the file *image.new* in slot 1 to the Flash memory card in PCMCIA slot 0.

Note Take this step only if sufficient space is available on the Flash memory card in slot 0 to hold both the new image and the old image already resident on the Flash memory card.

```
Router# copy slot1:image.new slot0:image.new
```

Entering this command in the following form will achieve the same result:

```
Router# copy slot1:image.new slot0:
```

Step 5 Enter the following commands to designate the file named *image.new* in the Flash memory card in slot 0 as the new default system image for boot purposes:

```
Router# configure terminal
Router(config)# no boot system
Router(config)# boot system flash slot0:image.new
Ctrl-Z
Router# copy running-config startup-config
Router# reload
```

When the system reloads, the file *image.new* is booted from the Flash memory card in slot 0.

Copying Files Between RP Memory and a Flash Memory Card

If you do not have access to a TFTP server where you can temporarily store a configuration file, you will need to copy a configuration file to a Flash memory card inserted in PCMCIA slot 0 or slot 1. You can then copy the configuration file back to NVRAM at any time. You can copy either your startup configuration file (from NVRAM) or your running configuration file (from DRAM).

Use the following procedures to first copy the configuration file from either NVRAM or DRAM to a Flash memory card, and to then copy the configuration file from a Flash memory card back to NVRAM:

- Copying Configuration Files from RP NVRAM to a Flash Memory Card, page 3-77
- Copying a Configuration File from RP DRAM to a Flash Memory Card, page 3-80
- Copying a Configuration File from a Flash Memory Card to RP NVRAM, page 3-81

Note You cannot copy files directly into DRAM.

Copying Configuration Files from RP NVRAM to a Flash Memory Card

Use the command **copy startup-config** [**slot0:** | **slot1:**] *filename* for the copy procedure, where **startup-config** is the source of the file (NVRAM), [**slot0:** | **slot1:**] is one of the Flash memory card slots, and *filename* is the name of the configuration file to be copied. Note that the environmental variable CONFIG_FILE must point to NVRAM (the system default).

To copy a configuration file named *myfile2* from the NVRAM on the RP to a Flash memory card in slot 0, follow these steps:

Step 1 Enter the **show bootvar** command at the privileged EXEC mode prompt to display the current setting for the CONFIG_FILE environmental variable, as follows:

```
Router# show bootvar
.
.
.
CONFIG_FILE variable =
Current CONFIG_FILE variable =
.
.
.
Router#
```

The absence of any notation following the CONFIG_FILE variable statement in this sample display indicates that the environmental variable points to NVRAM (the system default).

Step 2 To begin the copy operation, enter a **copy** command in the following form at the privileged EXEC mode prompt:

copy startup-config [**slot0:** | **slot1:**]*filename*

where

startup-config	Specifies the source of the file to be copied (NVRAM).
[**slot0:** | **slot1:**]*filename*	Specifies the destination of the file (the Flash memory card slot number) and the name of the new file.

An example of the **copy startup-config slot0:***filename* command follows:

```
Router# copy startup-config slot0:myfile2
20575008 bytes available on device slot0, proceed? [confirm]
Address or name of remote host [1.1.1.1]?
Loading new.image from 1.1.1.1 (via Ethernet0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 7799951/15599616 bytes]
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Router#
```

In this example, the exclamation points `(!)` appear as the source file is being downloaded to the destination device. The `CCCCC` characters indicate that a cyclic redundancy check (CRC) is being calculated during the downloading process. The CRC verifies that the file has been correctly downloaded to the Flash memory card inserted in PCMCIA slot 0 or the designated destination device.

You can also copy the running configuration (located in DRAM) to a Flash memory card, as shown in the "Copying a Configuration File from RP DRAM to a Flash Memory Card" section on page 3-80."

Step 3 To further verify that the configuration file was copied correctly to the Flash memory card in slot 0, enter the **dir** command:

```
Router# dir slot0:
-#- -length- -----date/time------ name
1   5200084  May 10 2002 19:24:12 gsr-p-mz.112-8
3   1215     May 10 2002 20:30:52 myfile1
4   6176844  May 10 2002 23:04:10 gsr-p-mz.112-8.1
5   1186     May 10 2002 16:56:50 myfile2

9197156 bytes available (11381148 bytes used)
Router#
```

Copying a Configuration File from RP DRAM to a Flash Memory Card

To copy the running configuration file from DRAM to a Flash memory card, follow these steps:

Step 1 Enter the command for copying a running configuration file from DRAM to a Flash memory card. The command takes the following form:

copy running-config [**slot0:**|**slot1:**]*filename*

where:

running-config	Specifies the DRAM source of the file to be copied.
[**slot0:** | **slot1:**]*filename*	Specifies the destination of the configuration file to be copied (the Flash memory card inserted in either slot 0 or slot 1) and the name of the new file.

An example of the **copy running-config slot0:***filename* command follows:

```
Router# copy running-config slot0:myfile2
20575008 bytes available on device slot0, proceed? [confirm]
Address or name of remote host [1.1.1.1]?
Loading new.image from 1.1.1.1 (via Ethernet0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!![OK - 7799951/15599616 bytes]
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Router#
```

In this example, the exclamation points `(!)` appear as the source file is being downloaded to the destination device. The `ccccc` characters indicate that a cyclic redundancy check (CRC) is being calculated during the downloading process. The CRC verifies that the file has been correctly downloaded to the Flash memory card inserted in PCMCIA slot 0 or the designated destination device.

Step 2 To further verify that the file was copied correctly, enter the **dir** command at the privileged EXEC mode prompt:

```
Router# dir slot0:
-#- -length- -----date/time------ name
1   5200084  May 10 2002 19:24:12 gsr-p-mz.112-8
3   1215     May 10 2002 20:30:52 myfile1
4   6176844  May 10 2002 23:04:10 gsr-p-mz.112-8.1
```

```
5   1186     May 10 2002 16:56:50 myfile2

9197156 bytes available (11381148 bytes used)
Router#
```

Copying a Configuration File from a Flash Memory Card to RP NVRAM

To copy a configuration file from a Flash memory card in PCMCIA slot 0 or slot 1 to NVRAM, follow these steps:

Step 1 Enter the command for copying a configuration file from a Flash memory card to NVRAM. This command takes the following form:

copy [**slot0:**|**slot1:**]*filename* **startup-config**

where:

[**slot0:** | **slot1:**]*filename*	Specifies the source of the configuration file to be copied (the Flash memory card in either PCMCIA slot 0 or slot 1) and the name of the new file.
startup-config	Specifies the destination (NVRAM) of the file to be copied.

To start the copy operation, enter the following command at the privileged EXEC mode prompt:

```
Router# copy slot0:myfile startup-config
[ok]
Router#
```

Step 2 Use the following command to ensure that the startup configuration file, now stored in NVRAM, becomes the default running configuration file:

```
Router# copy startup-config running-config
Router#
%SYS-5-CONFIG_I: Configured from memory by console
Router#
```

Locked Blocks in Flash Memory Cards

A locked block in Flash memory cards occurs when power is lost or a Flash memory card is removed from its PCMCIA slot on the RP during a write or erase operation.

When a block of Flash memory is locked, it cannot be written to or erased. Any attempt to do so will consistently fail at the block location. The only way to recover from locked blocks in a Flash memory card is to reformat the Flash memory card using the **format** command.

Caution Formatting a Flash memory card erases all existing data on the card.

If You Need More Information

If your router is not fully functional, you may need to perform additional configuration tasks. For more detailed information about configuring the router and its interfaces, see the publications listed in the following section.

The Cisco IOS software running your router contains extensive features and functionality. For information on Cisco IOS software and general installation and maintenance information for your router, use the following resources.

Cisco IOS Software Configuration Information and Support

The modular configuration and modular command reference publications in the Cisco IOS software configuration documentation set correspond to the Cisco IOS software release installed on your Cisco hardware. You can also see the Cisco IOS software release notes for the version of Cisco IOS software you are using on your router.

You can access Cisco IOS software documentation and hardware installation and maintenance documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

If you are reading Cisco documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** on the toolbar, and then select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

We appreciate your comments.

For information on regulatory compliance and safety, refer to *Regulatory Compliance and Safety Information for the Cisco 12000 Series Routers*, Document Number 78-4347-xx.

For additional line card information, refer to the installation and configuration note that accompanied your line card.

For additional GRP information, refer to the configuration note *Gigabit Route Processor (GRP) Installation and Configuration* (Document Number 78-4339-xx) that accompanied your GRP.

For additional PRP information, refer to the configuration note *Performance Route Processor (PRP) Installation and Configuration* (Document Number 78-13302-xx) that accompanied your PRP.

CHAPTER 4

Troubleshooting the Installation

This chapter provides troubleshooting guidelines for Cisco 12006 and Cisco 12406 Routers. If the solutions provided in this chapter do not make the router fully functional, contact your Cisco service representative for assistance.

Performing Other Configuration Tasks

This section describes the following additional configuration tasks.

Configuring the Software Configuration Register

The software configuration register is a 16-bit register in NVRAM that you use to define specific system parameters. You can set or change the contents of this register to accomplish the following tasks:

- Define boot sources for the default Cisco IOS software, assigning them in the following order of precedence:
  - Flash memory card inserted in PCMCIA slot 0
  - TFTP server on the network

  - Flash memory SIMM (NVRAM) on the RP
  - Boot image stored within the operating environment, which you access by using an appropriate form of the **boot** command entered at the ROM monitor prompt (`rommon>`)
- Define a default boot filename.
- Enable or disable the Break function.
- Control broadcast addresses.
- Set the console terminal baud rate.
- Force an automatic boot using a boot image.

  When you first power on the router, a boot image called the RP ROM monitor is executed, and the ROM monitor prompt (`rommon>`) is displayed. At this prompt, you have access to a limited set of commands that enable you to set values in the software configuration register and to perform other tasks.

  The RP ROM monitor is loaded into the RP Flash ROM when the RP is manufactured. You can use it to boot the system from local Flash memory devices. The RP ROM monitor software can be upgraded in the field, if necessary.
- Read **boot system** commands from the configuration file stored in NVRAM. Table 4-1 defines the bits in the software configuration register.

Caution To avoid confusion and possibly halting the system, remember that valid software configuration register values may be combinations of settings, rather than the individual settings listed in Table 4-1. For example, the factory default value 0x0102 for the software configuration register is a composite of several settings.

Table 4-1 Software Configuration Register Bit Meanings

Bit Number[1]	Hexadecimal Value	Definition/Function
00 to 03	0x0000 to 0x000F	Comprises the boot field for defining the source of a default Cisco IOS software image required to run the router
06	0x0040	Causes system software to ignore the contents of NVRAM

Table 4-1 Software Configuration Register Bit Meanings (continued)

Bit Number[1]	Hexadecimal Value	Definition/Function
07	0x0080	Enables the OEM[2] bit
08	0x0100	Disables the Break function
09	0x0200	Uses a secondary bootstrap
10	0x0400	Broadcasts Internet Protocol (IP) with all zeros
11 and 12	0x0800 to 0x1000	Defines the console baud rate (the default setting is 9600 bps)
13	0x2000	Boots the default Flash memory software if the network boot fails
14	0x4000	Excludes network numbers from IP broadcasts
15	0x8000	Enables diagnostic messages and ignores the contents of NVRAM

1. The factory default value for the software configuration register is 0x0102. This value is a combination of binary bit 8 = 0x0100 and binary bits 00 through 03 = 0x0002.
2. OEM = original equipment manufacturer.

Table 4-2 specifies the content of the *boot field*, which defines a source for booting the default Cisco IOS software image required to run the router. The content of the boot field is specified as a binary number.

Table 4-2 Boot Field and Meanings

Boot Field	Definition
00	On power up, the system remains at the ROM monitor prompt (`rommon>`) awaiting a user command to boot the system manually.
01	On power up, the system automatically boots the first system image found in the onboard Flash memory SIMM on the RP.

Table 4-2 Boot Field and Meanings (continued)

Boot Field	Definition
02 to 0F	On power up, the system boots automatically from a default Cisco IOS software image stored on a TFTP server in the network. For this setting, it is assumed that the Ethernet port on the RP is configured and operational. This setting also enables **boot system** commands that override the default filename.

Note Note: A Cisco 12006 or Cisco 12406 Router is typically delivered from the factory with a boot image in the boot flash and a Flash card containing a suitable working Cisco IOS image. If you need a Cisco IOS upgrade, you should FTP the appropriate Cisco IOS image from CCO.

Boot Field Settings

The four low-order bits of the software configuration register (bits 3, 2, 1, and 0) form a *boot field* that defines the source of a Cisco IOS software image for booting the router. You can set or change the contents of the boot field by issuing the **config-register** command at the global configuration mode prompt [`router(config)#`].

Note The factory default configuration register setting for an RP shipped in a router or an RP shipped as a field-replaceable unit is 0x0102.

When the boot field is set to either 0 or 1 (0000 or 0001), the system ignores any boot instructions in the system configuration file and one of the following occurs, depending on the boot field setting:

- When the boot field is set to 0, you must boot the operating system manually by entering the **boot** command at the ROM monitor prompt (`rommon>`). You can enter the **boot** command with or without arguments.

  If you enter the **boot** command *without* an argument (that is, without specifying a file or any other boot instructions), the system automatically boots using the default image in the Flash memory SIMM on the RP.

If you enter the **boot** command *with* arguments (that is, by instructing the system to boot from a specific source), you have these options:

- You can instruct the system to boot from a specific Flash SIMM image by entering the **boot bootflash:***filename* command, or from a specific image stored on a PCMCIA Flash memory card by entering the **boot slot #:** *imagename* command.
- You can instruct the system to boot from a network TFTP server either by sending broadcast TFTP requests by entering a **boot** *filename* command, or by sending a direct request to a specific network TFTP server by issuing a **boot** *filename ip-address* command.

- When the boot field is set to 1, the system automatically boots using the first image found in the onboard Flash SIMM on the RP.
- When the boot field is set to a bit pattern other than 0 or 1, the router uses the software configuration register settings to compute the filename of a default system image stored on a network TFTP server. It then uses that system image to boot the router. But if the configuration file contains boot instructions, the system uses these instructions to boot the system, rather than using the filename it computed from the software configuration register settings.

  To form this filename, the system starts with *cisco* and links the octal equivalent of the boot field value and the processor type in this format:

  cisco<*bootfieldvalue*>-<*processorname*>

  For example, the filename formation process would yield a range of filenames such as the following:

```
cisco2-grp
.
.
.
cisco17-grp
```

or

```
cisco2-prp
.
.
.
cisco17-prp
```

The system would use one of the filenames in this range to boot a default system image stored on a network TFTP server.

Note If a bootable Cisco IOS software image exists in a Flash memory card inserted in PCMCIA slot 0 or slot 1, the software configuration register boot field setting is overridden. The system then boots from the Cisco IOS software image in the Flash memory card, rather than from a network TFTP image (that is, from a computed filename in the range from *cisco2-grp* through *cisco17-grp* or *cisco2-prp* through *cisco17-prp*).

Configuration Register Settings

To change the software configuration register settings while running system software, follow these steps:

Step 1 Enter the **enable** command and your password at the user EXEC mode prompt to enter privileged EXEC mode:

```
Router> enable
Password: <password>
Router#
```

Step 2 Enter the **configure terminal** command at the privileged EXEC mode prompt on the system console to enter global configuration mode, as shown in the following example:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Step 3 Set the contents of the software configuration register by entering the **config-register** *value* command at the global configuration mode prompt, where *value* is a hexadecimal number preceded by 0x, as in the following:

```
Router(config)# config-register 0xvalue
```

Consult the hexadecimal column in Table 4-1 on page 4-2 for the possible settings to enter as the four-bit *value* parameter.

Step 4 Exit global configuration mode by entering **Ctrl-Z**.

```
Router(config)# config-register 0xvalue
Router(config)# Ctrl-Z
Router#
```

This command sequence saves the new contents of the software configuration register to NVRAM, but these new settings do not take effect until you reload or reboot the router.

Step 5 Enter the **show version** privileged EXEC command to display the software configuration register value currently in effect. This value will be used the next time the router reloads. The value is displayed on the last line of the screen display, as in the following example:

```
Router# show version

.
.
.

Configuration register is 0x141 (will be 0x102 at next reload)
```

Step 6 Save the software configuration register settings as described in the "Problem Solving with Subsystems" section on page 4-14.

Note Configuration register changes take effect only after the system reloads, such as when you enter a **reload** command from the console.

Step 7 Reboot the router.

Bits in the Software Configuration Register

This section provides more detailed descriptions of the significance of the bits in the software configuration register and how they interact during the boot process.

As described in the "Boot Field Settings" section on page 4-4, the boot field setting determines the source of the Cisco IOS software image that is used to boot the router. If you set the boot field value to 0 (0x0000), you must boot the operating system manually by entering the **boot** command at the ROM monitor prompt (`rommon>`) on the system console.

If you set the boot field value to 0x2 through 0xF and a valid **boot system** command is stored in the configuration file, the router boots the Cisco IOS software image as directed by that value. If no **boot system** command is present in the configuration file, the router forms a default boot filename and attempts to acquire that file from a network TFTP server.

In the following example, the software configuration register is set to boot the router from the Flash memory SIMM on the RP and to ignore the Break function at the next reboot of the system:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# config-register 0x0102
Router(config)# boot system flash filename
Ctrl-Z
Router#
```

With the configuration register set to 0x0102, the system computes a default boot filename. In forming this filename, the system starts with *cisco* and appends the octal equivalent of the boot field number, a hyphen, and the processor type (*grp* or *prp*).

Table 4-3 lists the range of possible computed default filenames for booting over the network. However, a valid **boot system** configuration command stored in the NVRAM configuration file overrides any computed default filename for booting over the network.

Note If a bootable Cisco IOS software image exists in a Flash memory card installed in PCMCIA slot 0 or 1, the configuration register setting is overridden, and the bootable Cisco IOS software image will be booted instead of the default TFTP-bootable Cisco IOS software image (*cisco2-grp* through *cisco17-grp* or *cisco2-prp* through *cisco17-prp*).

Table 4-3 Default Boot Filenames

Action/Filename	Bit 3	Bit 2	Bit 1	Bit 0
Bootstrap mode	0	0	0	0
Default software	0	0	0	1
cisco2-grp or cisco2-prp	0	0	1	0
cisco3-grp or cisco3-prp	0	0	1	1
cisco4-grp or cisco4-prp	0	1	0	0
cisco5-grp or cisco5-prp	0	1	0	1
cisco6-grp or cisco6-prp	0	1	1	0
cisco7-grp or cisco7-prp	0	1	1	1
cisco10-grp or cisco10-prp	1	0	0	0
cisco11-grp or cisco11-prp	1	0	0	1
cisco12-grp or cisco12-prp	1	0	1	0
cisco13-grp or cisco13-prp	1	0	1	1
cisco14-grp or cisco14-prp	1	1	0	0
cisco15-grp or cisco15-prp	1	1	0	1
cisco16-grp or cisco16-prp	1	1	1	0
cisco17-grp or cisco17-prp	1	1	1	1

The significance of bits 8 through 14 in the software configuration register follows.

Bit 8—Bit 8 of the software configuration register controls the console Break key. Setting bit 8 causes the system to ignore the console Break key. This is the factory default. Conversely, clearing bit 8 causes the system to interpret a Break keystroke as a command to halt normal system operation and force the system into ROM monitor mode. Regardless of the setting of the Break enable bit in the software configuration register, pressing the Break key during approximately the first 5 seconds of booting causes a return to the ROM monitor.

Bit 9—Bit 9 is not used.

Bits 10 and 14—Bit 10 of the software configuration register controls the host portion of the IP broadcast address. Setting bit 10 causes the processor to use all zeros in the host portion of the IP broadcast address; clearing bit 10 (the factory default) causes the processor to use all ones. Bit 10 interacts with bit 14, which controls the network and subnet portions of the IP broadcast address. Table 4-4 shows the combined effect of bits 10 and 14.

Table 4-4 Configuration Register Settings for Broadcast Address Destination

Bit 10	Bit 14	Address (<net> <host>)
Off	Off	<ones> <ones>
On	Off	<zeros> <zeros>
On	On	<net> <zeros>
Off	On	<net> <ones>

Bits 11 and 12—Bits 11 and 12 of the software configuration register determine the data transmission rate of the console terminal. Table 4-5 shows the bit settings for the four available data transmission rates. The factory-set default data transmission rate is 9600 bps.

Table 4-5 System Console Terminal Data Transmission Rate Settings

Bit 12	Bit 11	Data Transmission Rate (bps)
0	0	9600
0	1	4800
1	0	1200
1	1	2400

Bit 13—Bit 13 of the software configuration register determines the system response to a bootload failure. Setting bit 13 causes the system to load Cisco IOS software from Flash memory after five unsuccessful attempts to load a boot file from the network TFTP server. Clearing bit 13 causes the system to continue attempting to load a boot file from the network TFTP server indefinitely. Bit 13 is set to 0 as the default at the factory.

Recovering a Lost Password

This section provides information on how to recover a lost password.

Note If the enable password is encrypted, the following procedure will not work for password recovery, and you will have to reconfigure the system before attempting a reboot. To reconfigure the system, use the displayed configuration, which is shown using the **show startup-config** command in privileged EXEC mode, shown in Step 11.

To recover a lost password, follow these steps:

Step 1 Attach an ASCII terminal to the RP console port.

Step 2 Configure the terminal to operate at 9600 bps, 8 data bits, no parity, 2 stop bits (or whatever settings the console port is set to).

Step 3 Enter the **show version** command at the privileged EXEC mode prompt to display the existing software configuration register value.

```
Router# show version

.
.
.
```

The current configuration setting appears in the last line of the **show version** command output. Write this value on paper for use in Step 13.

Step 4 If the Break function is disabled, turn off power to the power supplies, wait 5 seconds, then restore power.

If the Break function is enabled, press the Break key or send a break by holding down the Control key and pressing the right square bracket key (Ctrl-]).

Step 5 Within 5 seconds of turning on the router, press the Break key. This action causes the terminal to display the ROM monitor prompt, as follows:

```
rommon 1>
```

Step 6 Set the software configuration register to ignore the configuration file information, as indicated in the following sample display:

```
rommon 1> config-register

    Configuration Summary
enabled are:
console baud: 9600
boot: image specified by the boot system command
or default to: cisco2-grp

do you wish to change the configuration? y/n [n]: y
enable "diagnostic mode"? y/n [n]:
enable "use net in IP bcast address"? y/n [n]:
enable "load rom after netbootfails"? y/n [n]:
enable "use all zero broadcast"? y/n [n]:
enable "break/abort has effect?" y/n [n]:
enable "ignore system config info?" [n]: y
change console baud rate? y/n [n]:
change boot characteristics? y/n [n]

Configuration Summary
enabled are:
console baud: 9600
boot: image specified by the boot system command
    or default to: cisco2-grp

do you wish to change the configuration? y/n [n]

You must reset or power cycle for the new config to take effect
rommon 1>
```

Step 7 Initialize the router by entering the **initialize** command at the ROM monitor prompt:

```
rommon 1> initialize
```

The router goes through a power cycle. The software configuration register is set to ignore the configuration file.

Step 8 Enter **no** in response to the system configuration dialog prompts until the following instruction is displayed:

```
Press RETURN to get started!
```

Step 9 Press **Return**.

After some interface configuration information is displayed, the user EXEC mode prompt appears:

```
router>
```

Step 10 Enter the **enable** command at the user EXEC mode prompt to enter privileged EXEC mode:

```
router> enable
Password: <password>
Router#
```

The prompt changes from `router>` to `router#` (`>` to `#`) indicates the change in command mode.

Step 11 Enter the **show startup-config** command at the privileged EXEC mode prompt to display the **enable** password in the configuration file.

```
router# show startup-config

.
.
.
```

Step 12 Enter the **configure terminal** command at the privileged EXEC mode prompt to enter global configuration mode:

```
router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#
```

Step 13 Change the software configuration register value back to its original value (noted in Step 3). Alternatively, change this value to 0x0102 (the factory default) by using the **config-register 0x***value* command:

```
router(config)# config-register 0xvalue
router(config)#
```

Value is a hexadecimal number preceded by **0x**, as in the following example:

```
router(config)# config-register 0x0102
```

Step 14 Exit global configuration mode by entering **Ctrl-Z**.

```
router(config)# Ctrl-Z
router#
```

Step 15 Reboot the router and use the recovered password with the **enable** command to gain access to the router.

Problem Solving with Subsystems

The key to solving problems in the system is to try to isolate the problem to a specific subsystem. The first step in solving startup problems is to compare what the system *is doing* to what it *should be doing*. Because a startup problem is usually attributable to a single component, it is more efficient to first isolate the problem to a subsystem rather than troubleshoot each component in the system.

For troubleshooting purposes, Cisco 12006 and Cisco 12406 Routers consist of the following subsystems:

- Power subsystem—Includes the following components:
  - AC-input or DC-input power distribution unit (PDU)
  - AC-input power supplies or DC-input power entry modules (PEMs). Cisco 12006 and Cisco 12406 Routers can be configured for source AC or source DC power. (You can not mix and match AC and DC power.)
  - Chassis backplane power distribution. The –48 VDC power from the power supplies is transferred to the chassis backplane, which distributes –48 VDC power to the cards in the card cages through the backplane connectors. The blower module receives power from the chassis backplane and passes MBus data back to the chassis backplane through a PDU connector.

    DC-to-DC converters on the two alarm cards convert –48 VDC to +5 VDC and put it back on the chassis backplane, where it is picked up to power the MBus modules on other cards and the blower module.
  - DC-to-DC converters. Each card in the router is equipped with DC-to-DC converters. These converters are controlled by the MBus module on each card. The DC-to-DC converters take –48 VDC and convert it into the voltages required by the card circuitry.

- Cooling subsystem—Consists of the blower module, which circulates air through the card cages to cool the cards, and the fan in each of the power modules, which circulates cooling air through the power module bays.
- Processor subsystem—Includes the RP, up to five line cards (when no optional, redundant RP is installed), and two alarm cards, which are located in the alarm card cage directly below the CSC card cage. The RP and the line cards are equipped with onboard processors. The RP downloads a copy of the Cisco IOS image to each line card processor. A line card or RP that is partially installed in the backplane might cause the system to hang and crash. The system uses two four-character alphanumeric LED displays (at one end of the faceplate on each line card and RP) to display status and error messages, which can help in troubleshooting.

Identifying Startup Problems

Startup problems are commonly caused by the power source or by a card that is not seated properly in the backplane. Although an overtemperature condition is unlikely at initial startup, the environmental monitoring functions are included here because they also monitor internal voltages.

When you start up the router for the first time, you should observe the startup sequence. The normal startup sequence is as follows:

- Each card in the system has an MBus module and at least one DC-DC converter. Each MBus module controls the DC-DC converter for its card. The MBus module receives direct current voltage directly from the power supplies through the backplane. When the power supply power switches are turned on, each MBus module boots from an onboard electrically erasable programmable read-only memory (EEPROM) device. Each MBus module processor reads a set of identification pins on the card to the backplane connector. These pins tell the MBus module processor what kind of card it is mounted on, which determines how the MBus module will function.
- The clock and scheduler card (CSC), containing the system clock, immediately powers up.
- The MBus module on the RP monitors the progress of the CSC power up. When the CSC has powered up, the MBus module on the RP turns on its DC-DC converter, powering up the RP.

- The RP sends the instructions to each line card to power up. Each line card processor begins to perform its own boot process. Each line card, through its MBus module, notifies the RP when the boot process is complete.
- The RP sends a command to each switch fabric card to power up. As each switch fabric card powers up, its progress is monitored by its MBus module processor. When the power-up process is complete, the switch fabric card MBus module notifies the RP that the switch fabric card is online.
- As the boot process progresses for each card, the status of the card is displayed in the alphanumeric LED displays. The left display is powered by the DC-DC converter on the card; the right display is powered by the DC voltage that powers the MBus module.

Using LEDs to Gather Information

By checking the state of the LEDs on the power modules and the alphanumeric displays on the RP and line cards, you can determine when and where the system failed in the startup sequence.

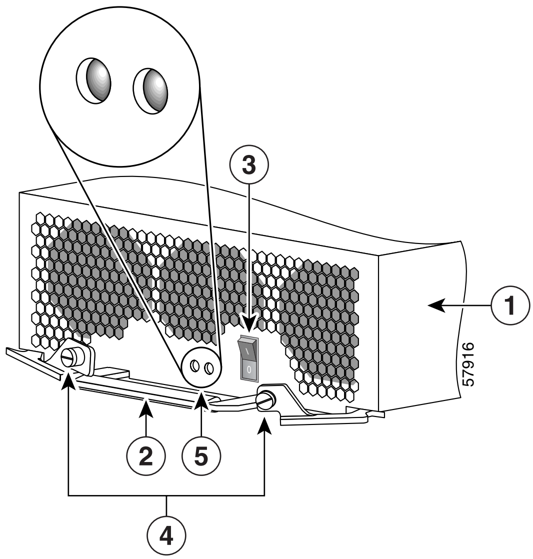
Note You can use the **test gsr led** IOS software command to perform an LED lamp test, which turns on all of the system LEDs at the same time for a specified period. This test allows you to verify that there are no failed LEDs.

The following sections describe what you should expect to see in the power module LEDs on router startup.

AC-Input Power Supply LEDs

Figure 4-1 shows the location of the LEDs on the power supply faceplate.

Figure 4-1 AC-Input Power Supply LEDs



1	AC-input power supply	**4**	Captive screws on release levers
2	Handle	**5**	LEDs
3	Power standby switch	**–**	–

Table 4-6 summarizes the function of these indicators.

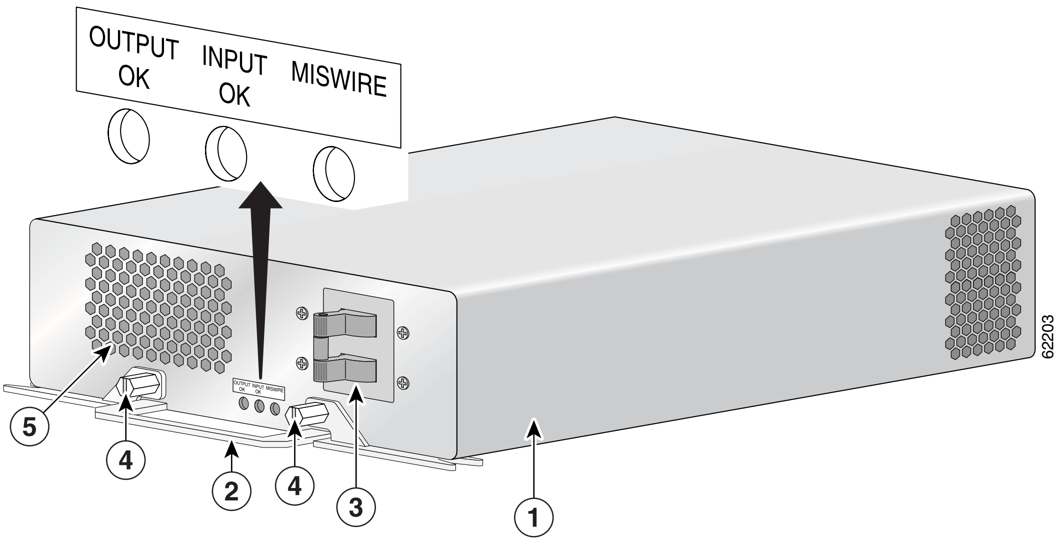
Table 4-6 AC-Input Power Supply LED indicators

LED Label	Function	State	Description
AC (Left LED)	Input power	On	AC power source is present and is within specified limits.
		Off	Power source is not within specified limits.
DC (Right LED)	Output Power	On	Power supply is operating normally in a power-on condition.
		Off	Power supply is operating in a fault condition and shutdown has occurred.

DC-Input Power Entry Module LEDs

Figure 4-2 shows the location of the LEDs on the DC-input PEM.

Figure 4-2 DC-Input Power Entry Module LEDs



1	DC-input PEM	**4**	Captive screws on release levers
2	Handle	**5**	Air inlet for cooling fan
3	ON/OFF switch	**–**	–

Table 4-7 summarizes the function of these indicators.

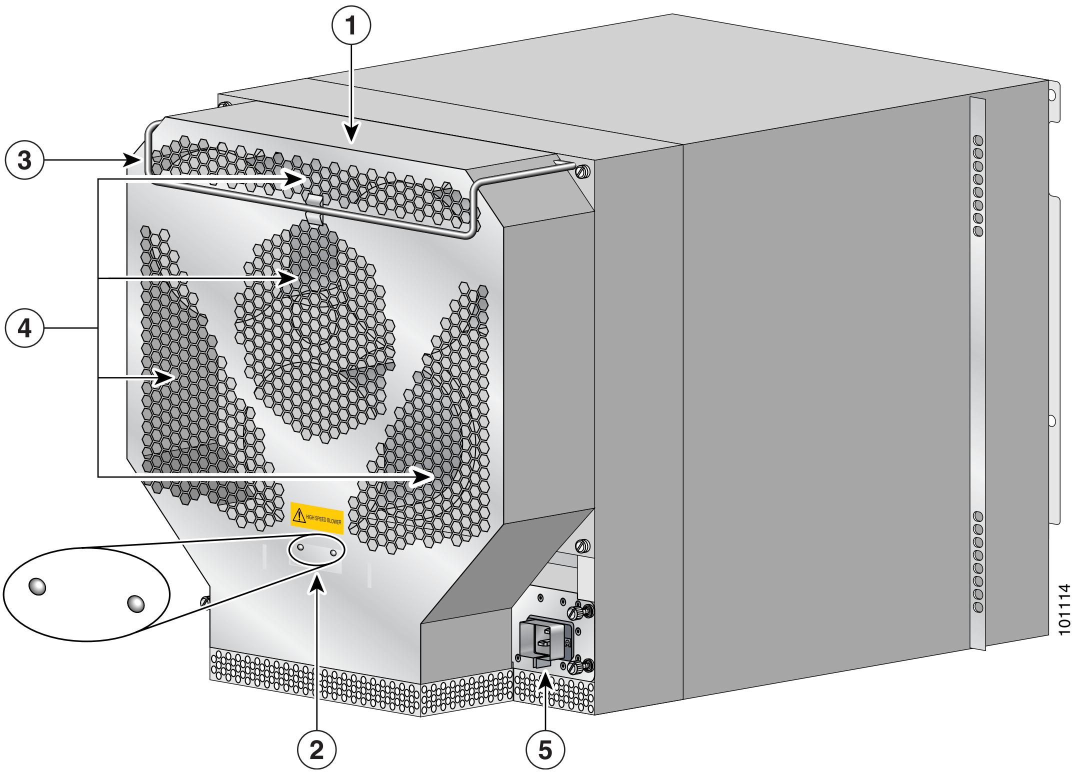
Table 4-7 DC-Input PEM LED Indicators

LED Label	Color	Function
OUTPUT OK	Green	PEM is operating normally in a powered-on condition.
INPUT OK	Green	DC power is present at the PEM input and within the specified limits.
MISWIRE	Amber	Indicates input is wired backward at the PDU input.

Blower Module LEDs

Figure 4-3 shows the location of the LEDs on the blower module.

Figure 4-3 Blower Module Location and Features



1	Blower module	**4**	Air exhaust vents
2	Blower module LEDs	**5**	Power distribution unit (PDU)
3	Blower module handle		

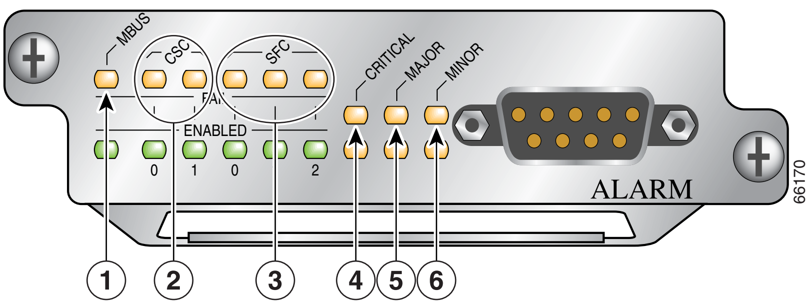
When the system is operating correctly, you should see these LED states:

- OK—Green. When on, the green OK LED indicates normal operation.
- FAIL—Off. When on, the red FAIL LED indicates the system has detected a fan failure or other fault in the blower module.The red LED should remain off during normal operation.

Alarm Card LEDs

Figure 4-4 shows the location of the LEDs on the faceplate of the alarm card.

Figure 4-4 Alarm Card LEDs



1	MBus status LED	**4**	Critical alarm LED
2	CSC status LEDs (two)	**5**	Major alarm LED
3	SFC status LEDs (three)	**6**	Minor alarm LED

When the system is operating correctly, the following LED conditions should be true.

LEDs that normally should be off:

- One MBUS status LED labeled FAIL
- Two CSC status LEDs labeled FAIL
- Three SFC status LEDs labeled FAIL
- Three router alarm LEDs labeled CRITICAL, MAJOR, MINOR

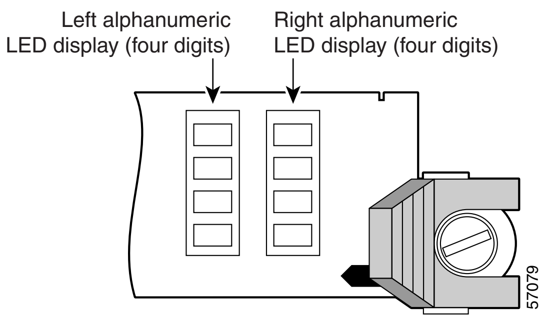
LEDs that normally should be on:

- One MBUS status LED labeled ENABLED
- Two CSC status LEDs labeled ENABLED
- Three SFC status LEDs labeled ENABLED

RP Alphanumeric LED Displays

Figure 4-5 shows the location of the alphanumeric LEDs on the RP faceplate.

Figure 4-5 RP Alphanumeric LED Displays (Partial Faceplate View)



When the router is powered on, the four-character alphanumeric displays on the RP indicate the following:

- Top display—Indicates which RP software component is running.
- Bottom display—Indicates the current phase of the boot process.

Status messages are displayed as the boot process continues. (See Table 4-8 on page 4-30.)

Troubleshooting the Power Subsystem

The power subsystem in the Cisco 12006 and Cisco 12406 Routers consists of the following components:

- An AC PDU or a DC PDU
- One or two AC-DC power supplies, or one or two DC-input PEMs
- Backplane
- DC-DC converters
- MBus modules

The power modules provide DC output to the system via the backplane. DC output from the alarm card powers the MBus modules on each card in the system. The MBus modules, in turn, control the DC-DC converters also present on each card in the system. The DC-DC converter takes DC power from the backplane and converts it into +2.5, +3.3, and +5 VDC, which is distributed to the card circuitry.

Begin checking the power subsystem by looking at the power module LEDs:

- For DC-input PEMs, see the "Troubleshooting the DC-Input Power Entry Module" section on page 4-26.
- For AC-input power supplies, see the following section.

Troubleshooting the AC-Input Power Subsystem

Begin checking the AC-input power subsystem by first looking at the LEDs on the AC-input power supplies (see the "AC-Input Power Supply LEDs" section on page 4-17). When you start up the system by turning on facility power to the system, the following should occur:

- The green LED labeled AC should go on immediately. It should remain on as long as the system is receiving satisfactory AC power levels from the facility AC power source.
- The green LED labeled DC indicates the status of the power module DC output power and internal DC voltages. This LED stays on when all the following conditions are met:
  - The power supply is fully seated in its bay.
  - The power supply power standby switch is on.

- For installations in North America, the AC input power range is between 100 and 240 VAC, with a 20A service. For international environments, the AC input power range is between 185 and 264 VAC, with a 16A service.
- Power supplies are providing –48 VDC to internal components.
- All internal DC voltages are within tolerance.

  If the AC power source or any of the power supply internal DC voltages exceed allowable tolerances, the DC LED will not go on, or will go off shortly after you turn on the power standby switch.

The power supplies are monitored by the MBus module and the RP for over- or undervoltage and over- or undercurrent conditions.

To help isolate a problem with an AC-input power supply, follow these steps:

Step 1 If the AC LED is off, verify that the power supply is fully seated in its bay, the ejector levers are flush with the power supply faceplate, and the captive screws are secured.

- If the AC LED goes on, go to Step 6.
- If the AC LED remains off, go to Step 2

Step 2 Check the AC power source.

a. Check the AC power cord from the power source to the router.

- Verify that the power cord is seated securely in the PDU and the AC outlet.
- Verify that the power cord is not worn or damaged. If the insulation appears cracked or broken, or the plugs appear loose, replace the power cord with a new power cord.

b. Verify that the AC power source circuit breaker is on and has not tripped, and that the circuit breaker has the proper current rating.

c. Verify that each power supply in the router is attached to a separate AC power source.

d. If the router is connected to an uninterruptable power supply (UPS), verify that the UPS is functioning correctly. Note that there might be a UPS for each power supply in the system.

If the AC power source wiring appears to be okay, but the power supply AC LED remains off, go to Step 3.

Step 3 Plug the power cord into a different, but compatible AC outlet.

- If the power supply AC LED goes on, the original AC outlet is faulty and cannot be used. Notify the appropriate facilities personnel and go to Step 6.
- If the power supply AC LED remains off, go to Step 4.

Step 4 Exchange the existing power cord for another power cord.

- If the power supply AC LED goes on, the original power cord is faulty and must be replaced. The AC portion of the power supply is working normally, go to Step 6.
- If the AC LED still fails to go on when connected to a different power source with a new power cord, the power supply is probably faulty. Go to Step 5.

Step 5 If a spare power supply is available, replace the existing module with the spare and restart the system.

- If the AC LED on the spare power supply goes on, the power supply is working normally, go to Step 6. The original power supply is faulty and should be returned for replacement.

Step 6 Is the power supply DC LED on?

- If Yes, the power supply is functioning normally. This is the end of the procedure.

Note In a Cisco 12006 or Cisco 12406 Router with two power supplies, the output power from the second power supply is adequate to maintain router operation, so the following check conditions only apply in a router with one power supply—or in a case where the second power supply is temporarily disabled by switching it off.

- If No, and there is no other system activity (blower module is off; line cards are unpowered), the power supply is faulty and must be replaced. Go to Step 7.
- If No, but the blower module is operating, suspect a faulty power supply DC LED. If the blower module is operating, all internal DC voltages are within tolerance. Use the **show environment** command to check the voltages on each card. The blower module uses –48 VDC.

Step 7 If a spare power supply is available, replace the existing module with the spare. If the DC LED then goes on, the power supply is working normally.

Return the faulty power supply for replacement.

If you are unable to resolve the problem or if you determine that either the power supply or power cable is faulty, contact a service representative for assistance.

Troubleshooting the DC-Input Power Entry Module

Begin checking the DC-input PEM by first looking at the LEDs on the PEM (see the "DC-Input Power Entry Module LEDs" section on page 4-19).

For a DC-input PEM to operate normally, the following conditions must be true:

- The PEM is fully seated in its bay and the ejector levers are secured.
- DC-input power within the required range is correctly connected to the chassis PDU terminal connector blocks.
- The circuit breaker on the faceplate of the PEM is switched on.
- The green LEDs labeled OUTPUT OK and INPUT OK on the PEM faceplate are on, and the yellow LED labeled MISWIRE is off.

To help isolate a problem with a DC-input PEM, follow these steps:

Step 1 Is the MISWIRE LED on?

- If Yes, the source DC positive and negative cable leads are connected in reverse order to the terminal connector block on the PDU.
- If No, go to Step 2.

Step 2 If the INPUT OK LED is off, verify that the PEM is fully seated in its bay, the ejector levers are flush with the PEM faceplate, and the captive screws are secured.

- If the INPUT OK LED goes on, go to Step 6.
- If the INPUT OK LED remains off, go to Step 3.

Step 3 Verify that the PEM circuit breaker switch is on.

- If No, switch it on. If the INPUT OK LED goes on, go to Step 6.

- If Yes, go to Step 4.

Step 4 Turn off the PEM circuit breaker switch and check the DC power source:

a. Check the DC power wires from the power source to the router.

- Verify that the power wires are fastened securely at the PDU and the DC source.
- Verify that the power wires are not worn or damaged. If the insulation appears cracked or broken, have the power wires replaced.

b. Verify that the DC power source circuit breaker is on, and that the circuit breaker has the proper current rating.

c. Verify that each PEM in the router is attached to a separate DC power source.

- If the DC power source wiring appears to be okay, and the PEM INPUT OK LED goes on when you switch on the PEM, go to Step 6.
- If the DC power source wiring appears to be okay, but the power supply INPUT OK LED remains off when you switch on the PEM, go to Step 5.

Step 5 Remove the PEM and insert it in the second bay in the router, or into a bay on another Cisco 12006 or Cisco 12406 Router.

- If the INPUT OK LED remains off, the PEM is faulty and must be replaced.
- If the INPUT OK LED goes on, the input portion of the PEM is working normally, go to Step 6.

Step 6 Is the OUTPUT OK LED on?

- If Yes, the power source is good and the PEM is operating normally. This is the end of the procedure.

Note In a Cisco 12006 or Cisco 12406 Router with two PEMs, the output power from the second PEM is adequate to maintain router operation, so the following check conditions only apply in a router with one PEM—or in a case where the second PEM is temporarily disabled by switching it off.

- If No, and there is no other system activity (blower module is off; line cards are unpowered), the PEM is faulty and must be replaced. Go to Step 7.
- If No, but the blower module is operating, suspect a faulty OUTPUT OK LED. If the blower module is operating, all internal DC voltages are within tolerance. Use the **show environment** command to check the voltages on each card. The blower module uses –48 VDC.

Step 7 If a spare PEM is available, replace the existing module with the spare. If the OUTPUT OK LED then goes on, the PEM is working normally.

Return the faulty PEM for replacement.

If you are unable to resolve the problem or if you determine that either the PEM or power wiring is faulty, contact a service representative for assistance.

Troubleshooting the Processor Subsystem

The Cisco 12006 and Cisco 12406 Router processor subsystem consists of the RP, the line cards, and the alarm cards. The RP and the line cards each have two processors. One processor is the main processor; the other processor is a component in the MBus module. The MBus module begins operation as soon as power is applied to the system. The MBus module determines the type of card it is mounted on and whether it should turn on the DC-DC converter. The RP MBus module turns on card power after a brief delay; the line card MBus modules delay turning on power until they receive a command from the RP.

A Cisco 12006 and Cisco 12406 Router requires that one RP be installed, or the system cannot operate. A line card that is partially connected to the backplane will send incomplete signals to the RP, which could cause the system to hang. Line cards should be completely installed and seated in the backplane connector, or fully removed and placed in a protective ESD device. If necessary, you can troubleshoot individual line cards, but first ensure that the RP is installed properly and the system software has initialized successfully.

A power-on self-test (POST) runs immediately at power-on to determine the condition of the RP memory. Results are displayed in the alphanumeric LED display as a pass/fail message.

Troubleshooting the RP

Check the following to help isolate a problem with the RP:

- Both the alphanumeric LED displays are on.

  The two displays are powered separately. The left display receives power from the DC-DC converter on the RP. The right display is powered directly from the power supply. If the RP is not powered up, its right display may be

on. If both displays are off, the RP may not be properly seated in the backplane connector. There also might be a problem with the MBus module on the RP, or the system power supply might be off.

- If both displays are on, check the message being displayed. As soon as the DC-DC converter is turned on by the MBus module, the processor on the RP begins the boot process. Status messages are displayed as the boot process continues. Table 4-8 provides a list of messages that can be displayed by the RP alphanumeric LED display. If one of the messages appears frozen, the boot process could be halted. Make a note of the message being displayed. Turn off the system power supply power switches, then turn them back on to reset the system. This starts the boot process again. If the system halts again, the RP could be faulty and might need to be replaced.
  - If the power modules and blower module appear operational, but none of the RP LEDs or displays are on, suspect that the RP has not been properly installed or that the +5 VDC output from the alarm card is faulty.
  - Turn the power switch to each power module to the OFF position.
  - Loosen the two captive screws on the left and right sides of the RP faceplate, and use the ejector levers to eject and reseat the RP. Tighten the captive screws, then power up the system by turning the power module power switches on.
- Is a critical, major, or minor alarm LED on the alarm card on?
  - If any of the three alarm card alarm LED pairs is on, a fault has been detected in the system. Check the console for messages indicating the source of the problem.
  - There could be a false error indication originating from the RP. You might want to reseat or replace the RP.

Caution The RP reset switch resets the RP and the entire system. To prevent system errors and problems, use it only at the direction of a Cisco-certified service representative.

Table 4-8 RP Alphanumeric LED Display Messages

LED Display[1]	Indications[2]
LMEM TEST	Low-memory test running
LCAH INIT	Lower 15k cache initialization
BSS INIT	Initialize main memory for ROM
NVRAM INIT	Initialize NVRAM
EXPT INIT	Initialize interrupt handlers
TLB INIT	Initialize TLB
CACH INIT	Initialize CPU data and instruction cache
CACH PARY	Enable CPU cache parity
MEM INIT	Initialize main memory
NVRAM SIZE	Size of the NVRAM
PCMC INIT	Initialize the PCMCIA
EXIT INIT	Exit the initialization sequence
IOS UP	The Cisco IOS software is up and running
MSTR RP	The RP is enabled and recognized by the system

1. The messages shown do not indicate a specific sequence.
2. Some messages appear for a fraction of a second; others last several seconds.

Troubleshooting the Line Cards

Line cards can be installed in slots in the card cage. As each line card powers up, a power-on self-test (POST) is performed on the line card memory. A full set of field diagnostics can also be run on a line card from the system console, providing a pass/fail message both in the line card alphanumeric LED display and on the system console.

To help isolate a problem with the line cards, visually check the two alphanumeric LED displays to determine whether both display banks are on.

The two displays are powered separately. The left display receives power from the DC-DC converter on the line card. The right display is powered directly from the backplane. Therefore, even if the line card has not powered up, the right display could be on. If both displays are off, the line card might not be fully plugged into the backplane connector, there might be a problem with the MBus module on the line card, or system power might be off.

If both displays are on, check the message being displayed. As soon as the DC-DC converter is turned on by the MBus module, the processor on the line card begins the boot process. Status messages are displayed in the alphanumeric displays as the boot process continues on the line card.

Table 4-9 provides a list of messages that can be displayed by the line card alphanumeric LED display. Some of these messages are displayed only for a fraction of a second; others last for several seconds.

Table 4-9 Line Card Alphanumeric LED Display Messages

LED Display[1]	Indications[2]
MEM TEST	POST memory test running
LROM RUN	POST memory test has finished running
BSS INIT	Initialize main memory for ROM
RST SAVE	Save reset reason register
IO RST	Reset the I/O system on the card

Table 4-9 Line Card Alphanumeric LED Display Messages (continued)

LED Display[1]	Indications[2]
EXPT INIT	Initialize interrupt handlers
TLB INIT	Initialize TLB
CACH INIT	Initialize CPU data and instruction cache
MEM INIT	Initialize main memory
LROM RDY	Ready to access download
ROMI GET	Getting ROM images
FABL WAIT	Wait for load of fabric downloader
FABL DNLD	The fabric downloader loads
FABL STRT	The fabric downloader launches
FABL RUN	The fabric downloader launch is complete
IOS DNLD	The Cisco IOS software downloads
IOS STRT	The Cisco IOS software launches
IOS UP	The Cisco IOS software runs in DRAM
IOS RUN	The line card is enabled and ready for use

1. The messages shown do not indicate a specific sequence.
2. Some messages appear only for a fraction of a second; others last several seconds.

Troubleshooting by Using the Alarm Cards

The alarm cards are installed in the alarm card slots immediately beneath the clock and scheduler card slots. The alarm card has four primary functions:

- Redundant generation of the DC MBus supply voltage for the line cards
- Power system monitoring functions
- OK/FAIL status indication of the CSCs and SFCs
- Hardware implementation of the alarm system relay outputs and indicators

The status of these functions is displayed in the LEDs on the faceplate of the alarm card. (See Figure 4-4.)

Monitoring Alarm Card Status

The alarm card faceplate has one pair of LEDs, labeled MBUS, that indicate the operational status of the alarm card.

A green MBUS LED labeled ENABLED indicates that the card has been detected by the system and is okay. A yellow MBUS LED labeled FAIL indicates that the system has detected a fault in the alarm card.

If no faults have been detected on an alarm card, the green MBUS LED labeled ENABLED should be on, and the yellow LED labeled FAIL should be off.

Monitoring Switch Fabric Status

If there are no faults on either CSC 0 or CSC 1, the green LED labeled ENABLED for each CSC should be on, and the yellow LED labeled FAIL for each CSC should be off. If the system detects a CSC fault, it turns off the green ENABLED LED for the faulty card, turns on the yellow FAIL LED, logs a warning message on the system console, and continues operating.

Note If the yellow LED labeled FAIL for a CSF or SFC is on, check the system console for messages describing the fault.

If there are no faults on the SFCs (SFC 0, SFC 1, or SFC 2), the green LED labeled ENABLED for each SFC should be on, and the yellow LED labeled FAIL for each SFC should be off. If the system detects an SFC fault, it turns off the green ENABLED LED for the faulty card, turns on the yellow FAIL LED, logs a warning message on the system console, and continues operating.

Monitoring Critical, Major, and Minor Alarm Status

The alarm card faceplate is equipped with three pairs of alarm status LEDs that are used to identify system alarm conditions detected through the MBus:

- Critical
- Major
- Minor

Note The LEDs are paired for redundancy to protect against a single failed LED. If any of the six LEDs is on, check the system console for messages describing the fault.

Because there are two alarm cards in a Cisco 12006 or Cisco 12406 Router, a system alarm condition detected through the MBus causes the same LEDs to be illuminated on both alarm cards.

The alarms can warn of an overtemperature condition on a component in one of the card cages, a fan failure in a blower module, an overcurrent condition in a power supply, or an out-of-tolerance voltage on one of the cards in one of the card cages. The LEDs are driven by MBus software, which sets the threshold levels for triggering the different stages of alarms.

The RP continuously polls the system for temperature, voltage, current, and fan speed values. If an over-threshold value is detected, the RP sets the appropriate alarm severity level on the alarm card, which lights one of the LED pairs on the alarm display and energizes the appropriate alarm display relays, activating any external audible or visual alarms wired to the alarm display. The RP also logs a message about the threshold violation on the system console.

Troubleshooting the Cooling Subsystem

Cisco 12006 and Cisco 12406 Routers have a blower module located on the rear of the chassis, which provides cooling air for the router components. (See Figure 4-3.)

The blower module receives power and signals though a connector recessed in the blower module. This connector mates with a connector mounted on the PDU. The blower module contains three fans, one connector, and one controller card. There are two LEDs on the blower module faceplate visible at the rear of the chassis.

- Green LED labeled OK—When on, this LED indicates that the blower module is functioning normally.
- Red LED labeled FAIL—When on, this LED indicates that the blower module is not functioning normally.

If the green LED is off and/or the red LED is on, check the following to help isolate a problem with the cooling system:

- Listen for the blower fans. In noisy environments, place your hand behind the blower module to feel for air being forced out the exhaust vents. If the blower module fans are on, the DC voltage from the power modules to the blower module is good.
- If the blower module fans are not on, there could a problem with either the blower module or the DC power from the power modules.
  - Check the output power LED on each power module (DC LED on the AC-input power supply; OUTPUT OK LED on a DC-input PEM). If the output power LED on a power module is off, but the input power LED is on, the power module might be faulty and should be checked or replaced.
  - If the output power LED on the power module is on (DC output is OK), but the blower module remains off, verify that the blower module is seated properly in the chassis.

    Remove the blower module by loosening the four captive screws holding it to the chassis, pull the blower module away from the chassis, then firmly push the blower module against the chassis to reseat the blower module. Tighten the four captive screws.
- If the blower module remains off, there could be a problem with the blower module controller card.

- The following console monitor message indicates that the system has detected an overtemperature or out-of-tolerance power condition in the router:

```
Queued messages:
%ENVM-1-SHUTDOWN: Environmental Monitor
initiated shutdown
```

  If an environmental shutdown results from an out-of-tolerance power condition, the output fail LED on the power module will go on before the system shuts down. Refer to the "Troubleshooting the Power Subsystem" section on page 4-23."

- Although overheating is unlikely at initial startup, be sure that heated exhaust air from other equipment is not entering the air filter, and that there is sufficient clearance—at least 6 inches (15.24 cm)— around the front and rear of the chassis to allow cooling air to enter and hot air to exhaust.
- Check the condition of the two air filters located in slots on the right side of the chassis. If the air filters appear dirty, remove the filters and either vacuum them or replace them.
- The preceding message could also indicate a faulty component or temperature sensor. Before the system shuts down, use the **show environment all** or **show environment table** command to display the internal system environment, including voltages and temperatures measured at each card.

If the blower module is faulty, you must replace the entire blower module.

If you are still unable to resolve the problem, contact a service representative for assistance.

CHAPTER 5

Field Diagnostics for the Cisco 12000 Series Router

Field diagnostics are available for all Cisco 12000 Series Routers to help you isolate faulty hardware to the level of a field-replaceable unit (FRU), without disrupting the operation of the system. After you identify the faulty unit, you can replace it with a spare unit.

Field diagnostics are not designed to identify specific components within the router. They simply determine whether a particular card is operational or defective.

Note Starting with Cisco IOS Release 12.0(22)S, the line card field diagnostics image is unbundled from the main Cisco IOS image. Line card field diagnostics are now stored and maintained as a separate image that must be available on a Flash memory card or TFTP boot server before the diagnostics commands can be used. Route processor and switch fabric card field diagnostics continue to be bundled and do not need to be launched from a separate image.

Unbundled field diagnostics offer the following benefits:

- In-service testing—Field diagnostics can be run on an in-service router running Cisco IOS and only take the card being tested out of service. If the tested card passes the diagnostic tests, it is returned to normal operation. If there is a hardware fault, the card remains out of service after the testing is completed.

- Smaller Cisco IOS image—To accommodate customers with 20-MB Flash memory cards, the line card field diagnostics are stored and maintained as a separate image that must be available on a Flash memory card or a TFTP boot server.
- Easy access to the most current diagnostics software—Since the field diagnostics software is now maintained as a separate image, the most recent version is always available on Cisco.com, without regard to the Cisco IOS software version currently in use.

The remainder of this chapter contains the following sections:

- Diagnostics Overview, page 5-2
- FPGA Overview, page 5-3
- Using Diagnostics, page 5-6
- Using the diag Command, page 5-8

Diagnostics Overview

There are more than 100 diagnostic operations for each Cisco 12000 Series Router line card, in addition to diagnostics for the switch fabric and route processor cards. These operations include the following:

- Processor tests
- Memory tests
- Component tests
- Major data path tests
- Field-programmable gate array (FPGA) image updates (on some line cards)

Note When using Cisco IOS Release 12.0(21)S or 12.0(21)ST or later, the default download method changes from the MBus to the switch fabric. It takes about 1 minute to obtain test results from the switch fabric, compared to 15 minutes to obtain test results from the MBus.

While diagnostics are running, the line card being tested is controlled by the diagnostic software. Diagnostics take the line card under test offline. The diagnostics affect just the line card being tested; the rest of the line cards remain online and continue to pass traffic normally. Diagnostics do not affect system performance.

Diagnostic testing stops when all the tests are completed, when testing is terminated by the user, or by default when an error is encountered. If multiple cards are specified for the test cycle, the diagnostics stop testing a card when it fails a test, but continue testing the remaining cards.

When testing is finished, a pass or fail message displays on the console, as well as on the alphanumeric LED display on the card being tested.

FPGA Overview

Some Cisco 12000 Series Router line cards store hardware information as software code in the form of a field-programmable gate array (FPGA). This code is permanently placed on Flash memory directly on the line card. Occasionally, this Flash memory code needs to be updated with a different FPGA code for feature enhancements or code improvements.

Some FPGA images are bundled within the Cisco IOS image and are updated along with a new release and do not require Flash memory storage. These FPGAs are likely to be those that are being developed and expanded within Cisco IOS feature sets. Others that are unlikely to undergo change are permanently stored in the Flash memory of the line card. Upon booting the line card, Cisco IOS may use an image bundled within itself, or it may access and use the FPGA image stored in Flash memory on the line card.

When the FPGA code resides on Flash memory and the Cisco IOS code checks the revision, you may be informed by the Cisco IOS boot process that an FPGA upgrade is necessary.

The following sample Cisco IOS boot text shows an FPGA upgrade message in bold text.

```
*Aug 19 14:51:06 UTC: %MBUS-6-FABCONFIG: Switch Cards 0x1F (bitmask)
    Primary Clock is CSC_1
    Fabric Clock is Redundant
    Bandwidth Mode : Full Bandwidth
    *Aug 19 14:51:23 UTC: %MBUS-6-NO_FPGA_IMG: FPGA image is not
appropriate or corrupted for slot 0. Please run Field Diagnostics
image on slot 0 to upgrade the FPGA image.
    *Aug 19 14:51:31 UTC: %GRPGE-6-SYNC_LOSS: Interface
GigabitEthernet2/0: Loss of Sync
    *Aug 19 14:51:31 UTC: %GRPGE-6-RX_LOS: Interface
GigabitEthernet2/0: Detected RX Loss of Signal
    SLOT 2:00:00:12: %SYS-5-RESTART: System restarted --
    Cisco Internetwork Operating System Software
    IOS (tm) GS Software (GLC1-LC-M), Experimental Version
12.0(20030605:093502) [mliflian-25-thr-work-nog-lke 115]
    Copyright (c) 1986-2003 by cisco Systems, Inc.
    Compiled Tue 19-Aug-03 17:33 by mliflian
```

When this message is received, the Cisco 12000 Series Router field diagnostics are used to update the Flash memory with the new image. When using field diagnostics to update the FPGA, no actual test is initiated, only an update to the FPGA code. See the “Upgrade the FPGA Image on a Line Card” section on page 5-7.

When field diagnostics run, the target line card stops passing traffic, but the rest of the router continues passing traffic normally. The line card is loaded with the field diagnostics program, the Flash memory update is run, and, if successful, the card reboots to Cisco IOS. The entire process takes approximately 2 minutes per line card and must be done one line card at a time. It is a good practice to wait about 30 seconds after Cisco IOS reloads on the line card before updating the next line card. This gives the router a chance to synchronize all its internal functions. The following sample output shows the process involved in updating the FPGA code on a line card in slot 0.

```
router# diag 0 verbose update-fpgas
    Running DIAG config check
    Fabric Download for Field Diags chosen: If timeout occurs, try
'mbus' option.
    Verbose mode: Test progress and errors will be displayed
    UUT will update FPGA's flash
    Running Diags will halt ALL activity on the requested
slot.[confirm]
    Router#
    Launching a Field Diagnostic for slot 0
```

```
    Loading muckier/award/c12k-fdiagsbflc-mz.conn_isp from
223.255.254.254 (via Ethernet0): !!!!!( stuff deleted)
    !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
    [OK - 8452824 bytes]


    FD 0> *****************************************************
    FD 0> GSR Field Diagnostics V6.14
    FD 0> Compiled by award on Mon Sep 22 14:05:20 PDT 2003
    FD 0> view: award-conn_isp.Field_Diag_Release
    FD 0> *****************************************************
    Executing all diagnostic tests in slot 0
    (total/indiv. timeout set to 3000/600 sec.)
    FD 0> BFR_CARD_TYPE_OC12_4P_ATM_E48 testing...
    FD 0> Available test types 2
    FD 0>                      1
    FD 0>                      3
    FD 0>                      11
    FD 0> Completed f_diags_board_discovery() (0x2f)
    FD 0> Verbosity now (0x00000211) TESTSDISP FATL IDSPRINTF
    FD 0> Test list selection received: Test ID 3, Device 0
    FD 0> running in slot 0 (1 tests from test list ID 3)
    FD 0> Skipping MBUS_FDIAG command from slot 5
    FD 0> Just into idle state
    FDIAG_STAT_IN_PROGRESS(0): test #1 Pinnacle FPGA Upgrade
    FD 0> Same version of IOB FPGA in flash and bundle: rev A0.79
    FD 0> IOB FPGA completed
    FD 0> MICKEY FPGA completed
    FD 0> Same version of MOUSE FPGA in flash and bundle: rev A0.11
    FD 0> MOUSE FPGA completed
    FD 0> Lower version of SAF FPGA being programmed over flash
bundle: Bundle rev B0.0A flash rev B1.10
    FD 0> SAF FPGA completed
    FD 0> Magic number indicates first use of this sector in flash for
CPK FPGA
    FD 0> WARNING: Not all devices flashed successfully:
fail_flag=0x0010
    FD 0> CPK FPGA completed
    FD 0> Displaying environmental information
    FD 0> 3.3V      5V     MBUS 5V  Hot Sensor   Inlet Sensor
    FD 0> (mv)     (mv)     (mv)     (deg C)       (deg C)
    FD 0> 3288     2568     5048      45.0          34.5
    FDIAG_STAT_DONE(0)


    FD 0> Changed current_status to FDIAG_STAT_IDLE
    Field Diagnostic ****PASSED**** for slot 0
```

```
    Field Diag eeprom values: run 8 fail mode 0 (PASS) slot 0
       last test failed was 0, error code 0
    Shutting down diags in slot 0


    Board will reload
    Router#
    Router#
    Router#
    SLOT 0:00:00:42: %SYS-5-RESTART: System restarted --
    Cisco Internetwork Operating System Software
    IOS (tm) GS Software (GLC1-LC-M), Experimental Version
12.0(20030909:221642) [hsiang-conn3 108]
    Copyright (c) 1986-2003 by cisco Systems, Inc.
    Compiled Thu 11-Sep-03 15:19 by hsiang
```

Using Diagnostics

Before proceeding with any diagnostics procedures, review the following:

- Obtain and Place the Diagnostics Image, page 5-6
- Upgrade the FPGA Image on a Line Card, page 5-7

Obtain and Place the Diagnostics Image

Before you can use the line card field diagnostics commands, you must obtain and place a valid diagnostics image on a separate Flash memory card installed in the router or on a TFTP boot server.

Field diagnostics images are approximately 18 MB in size. Cisco IOS images are slightly larger. A single 64-MB Flash memory card can contain both images, or these images can be stored individually on two 20-MB memory cards inserted into in card slot 0 and slot 1 on the RP. To accommodate future feature releases, it is recommended that you use larger Flash memory disks.

The diagnostics image is named **c12k-fdiagsbflc-mz.***120-25.S* and is always available on Cisco.com. 120-25.S is the version number of the image that corresponds to the Cisco IOS image, in this example, Cisco IOS Release 12.0(25)S.

Note All Cisco Systems field diagnostics images available on Cisco.com are backward and forward compatible with any Cisco IOS 12.0(22)S software release and later. Cisco strongly recommends always using the latest available field diagnostics image from Cisco.com for testing and verifying line cards.

Upgrade the FPGA Image on a Line Card

If a line card does not boot and you receive an error message indicating that there is a problem with the FPGA image, or if the line card alphanumeric LED display remains frozen in IOS STRT state, you need to upgrade the FPGA image using the **diag** command.

Note When the Cisco IOS image boots, it verifies that a compatible FPGA image is running on the router. The major version number of the FPGA image must be the same as that expected by the Cisco IOS image; the minor version number on the FPGA image must be the same as or greater than the minor version number expected by the Cisco IOS image. For example, if the Cisco IOS image expects a minimum FPGA image of 03.02, the software verifies that the actual major version number of the FPGA image in the line card bootflash is 03, and that the minor version number is 02 or above.

To upgrade the FPGA image on a line card, follow these steps:

Step 1 Enter privileged EXEC mode by entering the **enable** command followed by the password.

Step 2 Update the Flash memory with FPGA image(s) from the current field diagnostics download image by entering the **diag** command in this form:

diag *slot-number* **update-fpga source** {**tftp | flash**} *source-path*

The name of the image file is **c12k-fdiagsbflc-mz.***120-25.S,* where 120-25.S is the Cisco IOS Release number.

- For Flash memory cards, the source path would typically be **slot0:c12k-fdiagsbflc-mz.***120-25.S* or **slot1:c12k-fdiagsbflc-mz.***120-25.S*.

- For TFTP boot servers, the source path would typically be **tftp://***tftp_server_ip_address/my_directory***/c12k-fdiagsbflc-mz.***120-25.S*.

Caution Do not unplug the line card or terminate the field diagnostics session during this test.

Using the diag Command

To perform field diagnostics on a line card, route processor (RP) (including both the performance route processor [PRP] and gigabit route processor [GRP]), switch fabric card (SFC), or clock and scheduler card (CSC), use the **diag** command in privileged EXEC configuration mode. To halt a running field diagnostic session on a line card or RP, use the **diag halt** form of this command.

Caution Some line cards include components that are unable to isolate internal line card testing traffic from customer premise connections. When testing these line cards, you are warned and notified to disconnect any connections to these line cards before testing to achieve the most reliable results and minimize traffic disruption.

Cisco 12000 Series Router Line Cards

The following command examples apply to line card field diagnostics.

diag *slot-number* **source** {**tftp** | **flash**} *source-path* [**verbose**] [**wait**] [**full**] [**coe**] [**dl-timeout-plus** <*1-2000*>] [**device**] [**messaging**]

diag *slot-number* **previous**

diag *slot-number* **halt**

diag *slot-number* **update-fpga source** {**tftp** | **flash**} *source-path* [**dl-timeout-plus** <*1-2000*>]

Note Starting with Cisco IOS Release 12.0(22)S, the line card field diagnostics image is unbundled from the main Cisco IOS image. Line card field diagnostics are now stored and maintained as a separate image that must be available on a Flash memory card or TFTP boot server before the diagnostics commands can be used. Route processor and switch fabric card field diagnostics continue to be bundled and do not need to be launched from a separate image.

Cisco 12000 Series Router RPs

The following command examples apply to GRP and PRP field diagnostics:

diag *slot-number* [**verbose**] [**wait**] [**full**] [**coe**]

diag *slot-number* **previous**

diag *slot-number* **halt**

Cisco 12000 Series Router SFCs and CSCs

The following command example applies to SFC and CSC field diagnostics:

diag *slot-number* [**verbose**]

diag Command Reference

Table 5-1 lists the diag command options and their descriptions.

Table 5-1 diag Command Reference

Command	Description
slot-number	Slot number of the card you want to test.
source	Specifies that the source path of the line card diagnostic image follows. This keyword must be followed by either the **tftp** or **flash** keyword.

Table 5-1 diag Command Reference (continued)

Command	Description
tftp	Specifies that the source of the diagnostic image is a TFTP server. This keyword must be followed by the *source-path*. Also see the **dl-timeout-plus** option.
flash	Specifies that the source of the diagnostic image is a Flash memory card. This keyword must be followed by the *source-path*.
source-path	Path to the diagnostic image. The name of the image file is **c12k-fdiagsbflc-mz.***120-25.S*, where 120-25.S corresponds to Cisco IOS Release 12.0(25)S. For Flash cards, the source path would typically be **slot0:c12k-fdiagsbflc-mz.***120-25.S* or **slot1:c12k-fdiagsbflc-mz.***120-25.S*. The TFTP source path would typically be **tftp://***tftp_server_ip_address/my_directory***/c12k-fdiagsbflc-mz.***120-25.S*. This option is available and required for line card testing only.
halt	(Optional) Stops the field diagnostic testing on the line card. This option is only available for line cards and RPs.
previous	(Optional) Displays previous test results (if any) for the card. This option is only available for line cards and RPs.
verbose	(Optional) Enables progress and error messages to be displayed on the console. By default, only the minimum status messages are displayed on the console, along with the final result. Due to the comprehensive nature of testing, testing without the verbose option will result in up to a 15-minute delay before any results are displayed. Cisco recommends that the verbose option be specified and results captured when communicating with Cisco TAC.

Table 5-1 diag Command Reference (continued)

Command	Description
wait	(Optional) Stops the automatic reloading of the Cisco IOS software on the line card after the successful completion of the field diagnostic testing. If you use this keyword, you must use the microcode reload slot global configuration command, or manually remove and insert the line card (to power it up) in the slot so that the RP recognizes the line card and downloads the Cisco IOS software image to the line card.
coe	(Optional) Continue On Error. Normally the field diagnostics stop immediately upon failing any one test within a test session. Using the **coe** keyword forces the testing to continue to the end of the internal test list, even if a failure occurs. Caution should be exercised because in some cases where a cascade of failures is found, using this option MAY require the router to be reloaded, affecting all RPs and line cards. This option is only available for line cards and RPs.
full	(Optional) The default set of tests emphasize memory and data path tests. To force the line card or RP to complete the most extensive set of tests, use the full option. The test time will be slightly longer. This option is only available for line cards and RPs.
dl-timeout-plus **<1-2000** seconds**>**	(Optional) Allows you to manipulate the download timeout value. 300 seconds is the baseline value. Any value from 1 to 2000 adds that value to 300. For example, a **dl-timeout-plus** value of 12 makes the total value 312 seconds. Supports users with slow TFTP boot paths.

Table 5-1 diag Command Reference (continued)

Command	Description
update-fpga	(Optional) Updates flash memory with field-programmable gate array (FPGA) image(s) from the current field diagnostics download image. This option limits the field diagnostics session to one task: updating the FPGA images in flash memory on the line card. No other testing is performed during this session. This option updates ALL FPGA images in flash memory. This process is nonselective in cases where a line card contains multiple FPGAs. **Note** DO NOT unplug the line card or terminate the field diagnostics session during this test.
messaging	Provides additional troubleshooting information.

In some cases when field diagnostics indicates a card FAILURE, you may want to bring the line card back on line manually. In this case the **microcode reload** command may be used.

Caution Performing field diagnostics on a line card stops all activity on the line card. Before the **diag** command begins running diagnostics, you are prompted to confirm the request to perform field diagnostics on the line card.

In normal mode, if a test fails, the title of the failed test is displayed on the console. However, not all tests that are performed are displayed. To view all performed tests, use the **verbose** keyword.

After all diagnostic tests are completed on the line card, a PASSED or TEST FAILURE message is displayed. If the line card sends a PASSED message, the Cisco IOS software image on the line card is automatically reloaded unless the **wait** keyword is specified. If the line card sends a TEST FAILURE message, the Cisco IOS software image on the line card is not automatically reloaded.

If you want to reload the line card after it fails diagnostic testing, use the microcode **reload slot** global configuration command.

Note When you stop the field diagnostic test using the **diag halt** command, the line card remains down (in other words, in an unbooted state). Generally, you would stop testing in order to remove or replace the line card. If this is not the case, and you need to bring the line card back up (online), use the microcode **reload** global configuration command or power cycle the line card.

If the line card fails the test, the line card is defective and should be replaced. Under certain circumstances, Cisco Technical Assistance Center (TAC) engineers may direct you to replace field-replaceable memory modules and then retest. For example, if the DRAM test fails, you might only need to replace the DRAM on the line card. However, this should only be done under the guidance of a TAC engineer and only when observing tightly controlled static-sensitive device handling procedures. Do NOT replace memory components without proper body grounding and board grounding.

Output Examples

The following example shows the output when field diagnostics are performed on the line card in slot 7. After the line card passes all field diagnostic tests, the Cisco IOS software automatically reloads on the card. Before starting the diagnostic tests, you must confirm the request to perform these tests on the line card because all activity on the line card is halted. The *total/indiv. timeout set to 2000/600 sec.* message indicates that 2000 seconds are allowed to perform all field diagnostics tests, and that no single test should exceed 600 seconds to complete.

```
Router# diag 7 source tftp
tftp://192.164.5.4/images/c12k-fdiagsbflc-mz.120-25.S
Running DIAG config check
Fabric Download for Field Diags chosen: If timeout occurs, try 'mbus'
option.
Running Diags will halt ALL activity on the requested slot.  [confirm]
award-rp-slot0#
Launching a Field Diagnostic for slot 7
Downloading diagnostic tests to slot 7 via fabric (timeout set to 300
sec.)
5d20h: %GRP-4-RSTSLOT: Resetting the card in the slot: 7,Event:
EV_ADMIN_FDIAG
Loading images/award/c12k-fdiagsbflc-mz from 192.164.1.1 (via
Ethernet0):    !!!!!
5d20h: Downloading diags from tftp file
tftp://192.164.1.1/images/award/c12k-fdiagsbflc-mz
!!!!![OK - 13976524 bytes]
FD 7> *****************************************************
FD 7> GSR Field Diagnostics V6.05
FD 7> Compiled by award on Tue Jul 30 13:00:41 PDT 2002
FD 7> view: award-conn_isp.FieldDiagRelease
FD 7> *****************************************************
Executing all diagnostic tests in slot 7
(total/indiv. timeout set to 2000/600 sec.)
FD 7> BFR_CARD_TYPE_OC12_4P_POS testing...
FD 7> Available test types 2
FD 7>                      1
FD 7> Completed f_diags_board_discovery() (0x1)
FD 7> Test list selection received: Test ID 1, Device 0
FD 7> running in slot 7 (30 tests from test list ID 1)
FD 7> Skipping MBUS_FDIAG command from slot 2
FD 7> Just into idle state
Field Diagnostic ****PASSED**** for slot 7
Shutting down diags in slot 7
Board will reload
```

```
5d20h: %GRP-4-RSTSLOT: Resetting the card in the slot: 7,Event:
EV_ADMIN_FDIAG
SLOT 7:00:00:09: %SYS-5-RESTART: System restarted --
Cisco Internetwork Operating System Software
IOS (tm) GS Software (GLC1-LC-M), Experimental Version
12.0(20020509:045149)    [award-conn_isp.f_diag_new 337]
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Tue 25-Jun-02 15:51 by award
```

The following example shows the output of a line card test with the **verbose** option specified (highly recommended).

```
Router# diag 7 verbose tftp
tftp://192.164.1.1/images/award/c12k-fdiagsbflc-mz.120-25.S
Running DIAG config check
Fabric Download for Field Diags chosen: If timeout occurs, try 'mbus'
option.
Verbose mode: Test progress and errors will be displayed
Runnning Diags will halt ALL activity on the requested slot.
[confirm]
Router#
Launching a Field Diagnostic for slot 7
Downloading diagnostic tests to slot 7 via fabric (timeout set to 300
sec.)
00:07:41: %GRP-4-RSTSLOT: Resetting the card in the slot: 7,Event:
EV_ADMIN_FDIAG
Loading images/award/c12k-fdiagsbflc-mz from 192.164.1.1 (via
Ethernet0):      !!!!!! (...)
00:08:24: Downloading diags from tftp file
tftp://192.164.1.1/images/award/c12k-fdiagsbflc-mz
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!
[OK - 13976524 bytes]
FD 7> *****************************************************
FD 7> GSR Field Diagnostics V6.05
FD 7> Compiled by award on Tue Jul 30 13:00:41 PDT 2002
FD 7> view: award-conn_isp.FieldDiagRelease
FD 7> *****************************************************
Executing all diagnostic tests in slot 7
(total/indiv. timeout set to 2000/600 sec.)
FD 7> BFR_CARD_TYPE_OC12_4P_POS testing...
FD 7> Available test types 2
FD 7>                      1
FD 7> Completed f_diags_board_discovery() (0x1)
FD 7> Verbosity now (0x00000011) TESTSDISP FATL
FD 7> Test list selection received: Test ID 1, Device 0
FD 7> running in slot 7 (30 tests from test list ID 1)
FD 7> Just into idle state
```

```
FDIAG_STAT_IN_PROGRESS(7): test #1 Dram Marching Pattern
FDIAG_STAT_IN_PROGRESS(7): test #2 Dram Datapins
FDIAG_STAT_IN_PROGRESS(7): test #3 Dram Busfloat
FDIAG_STAT_IN_PROGRESS(7): test #4 RBM SDRAM Marching Pattern
FDIAG_STAT_IN_PROGRESS(7): test #5 RBM SDRAM Datapins
FDIAG_STAT_IN_PROGRESS(7): test #6 RBM SSRAM Marching Pattern
FDIAG_STAT_IN_PROGRESS(7): test #7 RBM SSRAM Datapins Memory
FDIAG_STAT_IN_PROGRESS(7): test #8 TBM SDRAM Marching Pattern
FDIAG_STAT_IN_PROGRESS(7): test #9 TBM SDRAM Datapins
FDIAG_STAT_IN_PROGRESS(7): test #10 TBM SSRAM Marching Pattern
FDIAG_STAT_IN_PROGRESS(7): test #11 TBM SSRAM Datapins Memory
FDIAG_STAT_IN_PROGRESS(7): test #12 PSA TLU SDRAM Marching Pattern
FDIAG_STAT_IN_PROGRESS(7): test #13 PSA TLU SDRAM Datapins
FDIAG_STAT_IN_PROGRESS(7): test #14 PSA PLU SDRAM Marching Pattern
FDIAG_STAT_IN_PROGRESS(7): test #15 PSA PLU SDRAM Datapins
FDIAG_STAT_IN_PROGRESS(7): test #16 PSA SRAM Marching Pattern
FDIAG_STAT_IN_PROGRESS(7): test #17 PSA SRAM Datapins
FDIAG_STAT_IN_PROGRESS(7): test #18 To Fabric SOP FIFO SRAM Memory
FDIAG_STAT_IN_PROGRESS(7): test #19 From Fabric SOP FIFO SRAM Memory
FDIAG_STAT_IN_PROGRESS(7): test #20 RBM to SALSA Packet
FDIAG_STAT_IN_PROGRESS(7): test #21 TBM to SALSA Packet
FDIAG_STAT_IN_PROGRESS(7): test #22 RBM to TBM SLI Packet Loopback
FDIAG_STAT_IN_PROGRESS(7): test #23 TBM to PSA Packet - Framer
Loopback
FDIAG_STAT_IN_PROGRESS(7): test #24 TBM to TX SOP Packet
FDIAG_STAT_IN_PROGRESS(7): test #25 TBM to RX SOP Packet - 4302
Terminal Loopback
FDIAG_STAT_IN_PROGRESS(7): test #26 TBM to RX SOP Packet - Framer
System Bus Loop
FDIAG_STAT_IN_PROGRESS(7): test #27 RBM to TBM Fabric Packet Loopback
FDIAG_STAT_IN_PROGRESS(7): test #28 TBM to RBM Packet, RBM page
crossing
FDIAG_STAT_IN_PROGRESS(7): test #29 TBM to TX SOP Packet Simultaneous
FDIAG_STAT_IN_PROGRESS(7): test #30 TBM to PSA Multicast Packets -
Framer Loopback
FDIAG_STAT_DONE(7)
FD 7> Changed current_status to FDIAG_STAT_IDLE
Field Diagnostic ****PASSED**** for slot 7
Field Diag eeprom values: run 62 fail mode 0 (PASS) slot 7
last test failed was 0, error code 0
Shutting down diags in slot 7
Board will reload
```

Following is an example of a test FAILURE condition on a GRP card. This card would need to be replaced and returned to Cisco for repair:

```
Field Diag download COMPLETE for slot 7
FD 3> *****************************************************
```

```
FD 3> GSR Field Diagnostics V6.01
FD 3> Compiled by award on Tue Apr 9 07:22:53 PDT 2002
FD 3> view: award-conn_isp.f_diag_new
FD 3> *****************************************************
Diagnostics have been downloaded to slot 7
Executing all diagnostic tests in slot 7
(total/indiv. timeout set to 2000/600 sec.)
FD 3> BFRP w/ECC testing...
FD 3> Secondary Discovery found ID 2
FD 3> BFR_CARD_TYPE_BFRP_CARD w/ ECC testing...
FD 3> Available test types 2
FD 3>                      1
FD 3> Completed f_diags_board_discovery() (0x1)
FD 3> Verbosity now (0x00000011) TESTSDISP FATL
FD 3> Test list selection received: Test ID 1, Device 0
FD 3> running in slot 7 (24 tests from test list ID 1)
FDIAG_STAT_IN_PROGRESS(3): test #1 BFRP Dram Datapins Test
FDIAG_STAT_IN_PROGRESS(3): test #2 Dram Marching Pattern Test
FDIAG_STAT_IN_PROGRESS(3): test #3 DataPins_Sram
FDIAG_STAT_IN_PROGRESS(3): test #4 March_Sram
FDIAG_STAT_IN_PROGRESS(3): test #5 High Memory DRAM Marching Pattern
FDIAG_STAT_IN_PROGRESS(3): test #6 diags_csar_regtest
FDIAG_STAT_IN_PROGRESS(3): test #7 diags_test_p4_csar_int
FDIAG_STAT_IN_PROGRESS(3): test #8 NVRAM Memory Test
FD 3> 32 bit data compare error. Wrote 0xcccccccc, read back
0xcc41cccc at location 0xbe03fff0
FDIAG_STAT_DONE_FAIL(3) test_num 8, error_code 1
COMPLETED Field Diags: pid 128, status 5, test_num 8, error_code 1
Field Diagnostic: ****TEST FAILURE**** slot 7: first test failed: 8,
NVRAM Memory Test, error 1
Field Diag results from eeprom before updating slot 7, run# 0x5000042
were 0x0
previous field diag eeprom values: run 66 fail mode 5 (DOWNLOAD
FAILURE)
last test failed was 0, error code 0
Field Diag eeprom values: run 67 fail mode 1 (TEST FAILURE) slot 7
last test failed was 8, error code 1
Shutting down diags in slot 7
slot 7 done, will not reload automatically
```

The following example shows the previous test results of a line card. Diagnostics had been run 64 times on this line card. Because the board PASSED the last field diagnostics session, the fail mode was 0 as was the last test that failed.

```
Router # diag 7 prev
Field Diag eeprom values: run 64 fail mode 0 (PASS) slot 7
   last test failed was 0, error code 0
```

The following example shows the output of a line card test with the **update-fpga** option specified.

```
Router# diag 7 verbose source tftp
tftp://223.255.254.254/c12k-fdiagsbflc-mz.120-25.S update-fpga
Running DIAG config check
Fabric Download for Field Diags chosen: If timeout occurs, try 'mbus'
option.
Verbose mode: Test progress and errors will be displayed
UUT will update FPGA's flash
Runnning Diags will halt ALL activity on the requested slot.
[confirm]
Router#
PID of f_diag_run is 121, set test_pid[3]
gdb slot is 0
Launching a Field Diagnostic for slot 7
Loading c12k-fdiagsbflc-mz.new_fpga from 223.255.254.254 (via
Ethernet0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Calling enable_slot_and_type_on_fabric(DISABLE) for slot 7
Calling enable_slot_and_type_on_fabric(ENABLE) for slot 7
FD 3> *****************************************************
FD 3> GSR Field Diagnostics V6.9
FD 3> Compiled by ckhuong on Fri Jan 17 15:51:36 PST 2003
FD 3> view: ckhuong-conn_isp.inti4
FD 3> *****************************************************
Diagnostics have been downloaded to slot 7
Executing all diagnostic tests in slot 7
(total/indiv. timeout set to 2000/600 sec.)
FD 3> BFR_CARD_TYPE_4P_GE_E48 testing...
FD 3> Available test types 2
FD 3>                      1
FD 3>                      3
FD 3>                      11
FD 3> Completed f_diags_board_discovery() (0x32)
FD 3> Verbosity now (0x00000011) TESTSDISP FATL
FD 3> Test list selection received: Test ID 3, Device 0
FD 3> running in slot 7 (1 tests from test list ID 3)
FD 3> Just into idle state
FDIAG_STAT_IN_PROGRESS(3): test #1 Tetra Flash Mem Upgrading
FD 3> Upgraded FPGA image in Flash from version 0xcc53 to 0xcc54
Calling enable_slot_and_type_on_fabric(DISABLE) for slot 7
Calling enable_slot_and_type_on_fabric(ENABLE) for slot 7
FDIAG_STAT_DONE(3)


FD 3> Changed current_status to FDIAG_STAT_IDLE
```

```
COMPLETED Field Diags: pid 121, status 6, test_num 1, error_code 0


Field Diagnostic ****PASSED**** for slot 7


Field Diag results from eeprom before updating slot 7, run# 0x10 were
0x0
previous field diag eeprom values: run 16 fail mode 0 (PASS)
   last test failed was 0, error code 0
Field Diag eeprom values: run 17 fail mode 0 (PASS) slot 7
   last test failed was 0, error code 0
Shutting down diags in slot 7


Board will reload
Router#
```

CHAPTER 6

Maintaining the Router

The Cisco 12006 or Cisco 12406 Router is equipped as ordered and is ready to install and start up when it leaves the factory. After you install and configure the router, you might need to perform other procedures to ensure that the router continues to operate properly. Also, as your networking requirements change, you might need to upgrade your system by adding or changing components.

This chapter describes how to maintain your router. The first section explains when and how to power down the router. The remaining sections describe the following maintenance procedures:

- Removing and Installing a Clock and Scheduler Card, Switch Fabric Card, or Alarm Card, page 6-56
- Removing and Installing the Chassis, page 6-68
- Upgrading the RP and Line Card Memory, page 6-77

Before performing the procedures in this chapter, review the safety information in the "Laser Safety" section on page 2-5 and the "Lifting Guidelines" section on page 2-5, and see the *Regulatory Compliance and Safety Information for the Cisco 12000 Series Router (*Document Number 78-4347-xx), which comes with your router.

Powering Down the Router

Unless otherwise noted, the maintenance tasks described in this chapter can be performed while the router remains powered on. Most Cisco 12006 and Cisco 12406 routers field replaceable units (FRUs) support online insertion and removal (OIR), which means they can be removed and installed (hot-swapped) while the router remains powered up.

- Line cards, switch fabric cards (SFCs), alarm cards, and the blower module are hot-swappable.
- Power modules, clock and scheduler cards (CSCs), and RPs also support OIR, but are hot-swappable only when the system is equipped with two power modules, two CSCs, or two RPs, respectively.
- The power distribution unit (PDU) does not support OIR.

To power down an AC- or a DC-powered router, follow these steps:

Step 1 Turn off the faceplate switches on the power modules.

Step 2 Turn off the facility circuit breakers for power source lines connected to the PDU.

Step 3 When the procedure requires that the router be disconnected from source power:

a. AC-powered systems—Unplug both AC power cords from the power outlets.

b. DC-powered systems—Disconnect and remove the source DC wires from both power connector blocks on the PDU.

Step 4 Verify that the following conditions are true:

a. LEDs on the power modules are off, and power module fans are off.

b. LEDs on the RP, line cards, and alarm cards are off.

c. LEDs on the blower module are off, and all blower module fans are off.

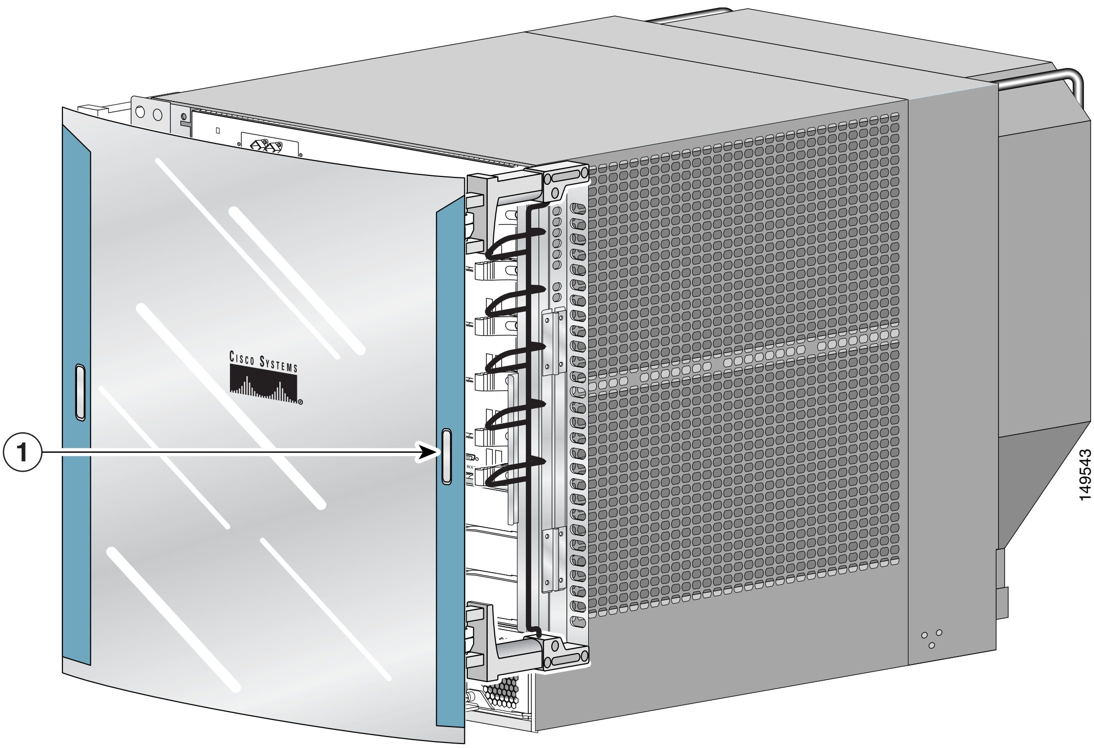
Removing and Installing the Front Door on Cisco 12006 and Cisco 12406 Enhanced Series Router

The Cisco 12006 and Cisco 12406 enhanced series routers have a new 1-piece front door. The router ships with the door hinge mounted on the left side of the chassis so that it opens from right-to-left. This section describes how to change the front door to open from left-to-right by installing the hinge on the opposite side.

Use the following procedure to change the location of the hinge.

Step 1 Open the front door by pressing the right latch button (Figure 6-1).

Figure 6-1 Opening the Front Door



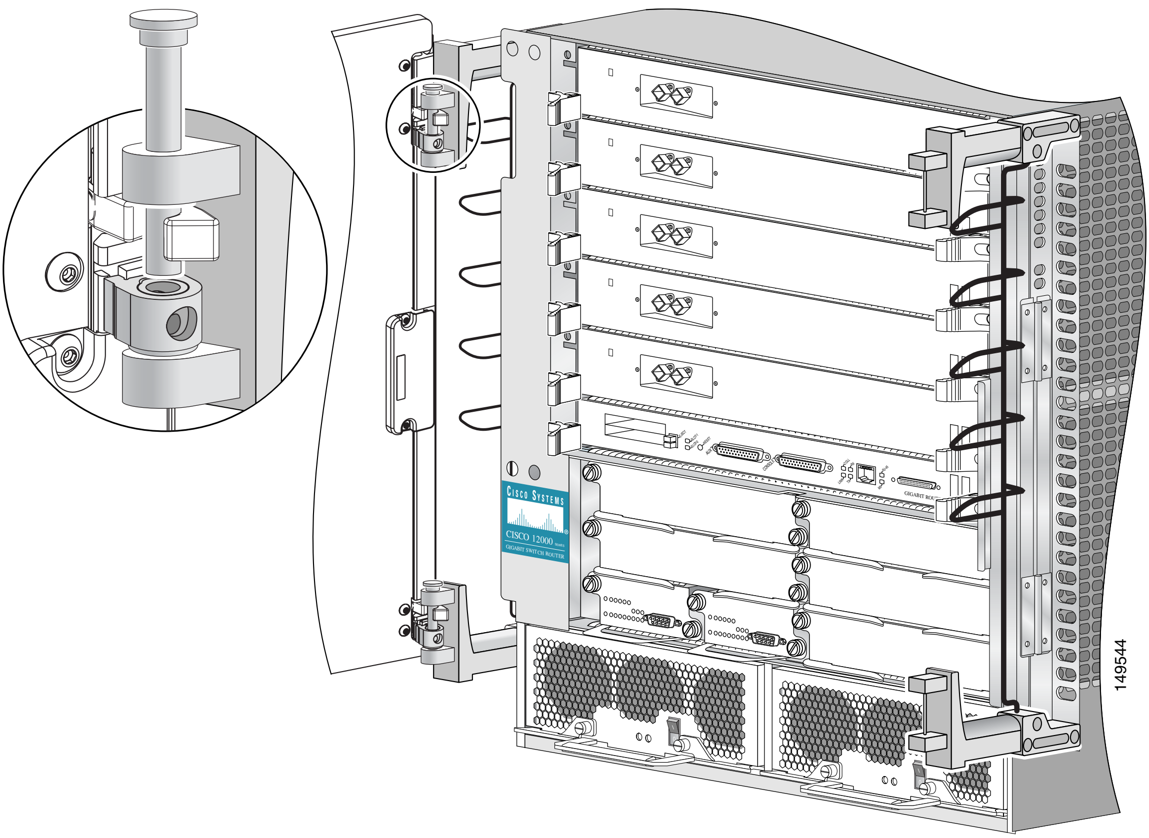
1	Front Door Latch

Step 2 Remove the front door by lifting the (top and bottom) hinge pins to free the door from the chassis (Figure 6-2).

Caution Make sure you are holding the front door securely so it does not drop when you release it from the chassis.

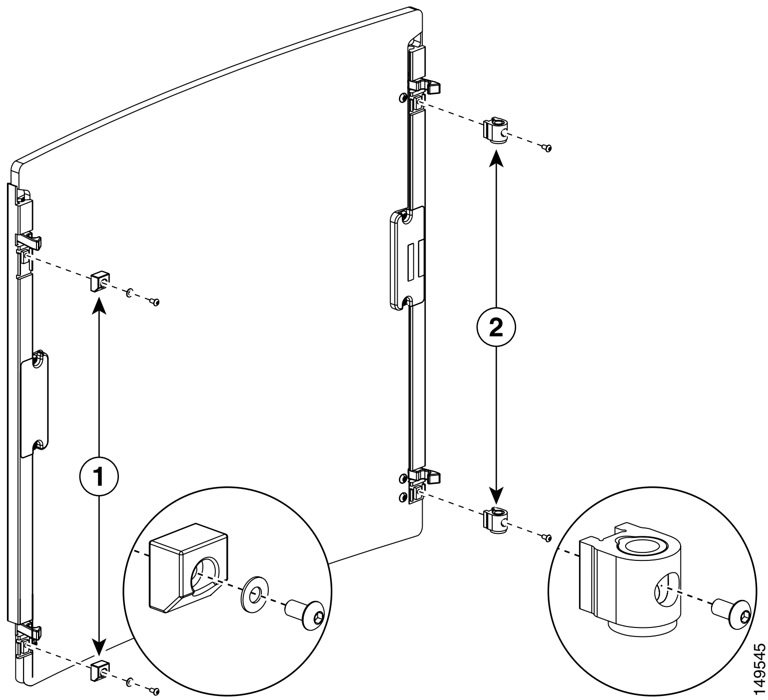
Step 3 Reinstall the hinge pins into the chassis hinge brackets.

Figure 6-2 Removing or Installing Hinge Pins



Step 4 Remove the bumpers and pivot blocks from the door as shown in Figure 6-3.

Figure 6-3 Removing the Bumpers and Pivot Blocks



1	**Bumpers**	**2**	**Pivot blocks**

Step 5 Reinstall the hardware to the opposite sides of the front door:

a. Mount pivot blocks to the left side and tighten the screws until snug.

b. Mount the bumpers to the right side and tighten the screws until snug.

Step 6 Attach the front door to the chassis:

a. Remove the hinge pins from the hinges on the right side of the chassis.

b. Align the pivot blocks on the front door with the hinges on the right side of the chassis and install the hinge pins to hold the door in place (see Figure 6-2).

c. Close the front door by pressing the latch button allowing the door latch to engage with the hinge pins on the chassis.

Cleaning or Replacing the Air Filters

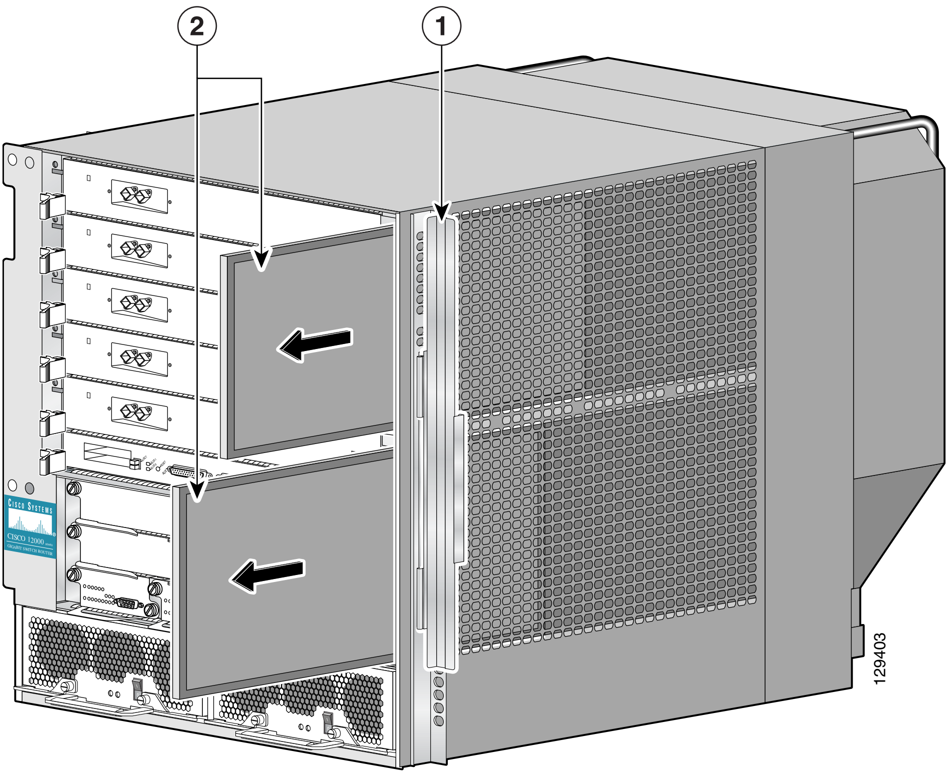
The Cisco 12006 and Cisco 12406 routers are equipped with two user-serviceable air filters that remove dust drawn into the router by the blower module. One time per month (or more often in dusty environments), examine the air filters.

Use the following procedure to clean or replace the air filters.

Step 1 Open the spring-loaded air filter door on the right side of the chassis and remove an air filter by pulling the small tab on the edge of the filter (Figure 6-4).

Remove the second air filter the same way.

Figure 6-4 Removing the Air Filters



1	Air filter door	**2**	Air filters

Step 2 Visually check the condition of the air filters to determine whether to clean them or install new replacements.

- Dirty—You can vacuum or replace the filters.

Caution Do not try to vacuum the air filter while it is installed in the chassis. You must remove the air filter completely before you clean it to prevent contaminants from being drawn into the router.

- Worn or torn—If the filters appear worn or torn, dispose of them in a responsible manner and install replacement air filters (ACS-GSR6-FLTR=).

Step 3 Open the air filter door and install the new or cleaned air filters.

Note An arrow located on the edge of each air filter frame that indicates the direction of *air flow*. Always install the air filter with the arrow pointing in toward the RP and line card cage.

Removing and Replacing the Blower Module

The illustrations in this procedure represent both the original and newer enhanced capacity blower modules for the Cisco 12006 and Cisco 12406 series routers; blowers that shipped with original systems, and enhanced capacity blowers that ship with current systems. If you are replacing an:

- Original blower module (GSR6-BLOWER=)—Use an original blower module *or* an enhanced capacity blower module as a replacement.
- Enhanced capacity blower module (12000/6-BLOWER=)—Use an enhanced capacity blower module as a replacement.

Note Compared to the original blower modules that shipped with Cisco 12006 and Cisco 12406 series routers, airflow capacity for new enhanced blower modules is increased by nearly 40 percent to provide additional cooling to the chassis. The new fans operate at a higher speed to provide improved airflow, so you may notice increased sound generated from the new blower module.

Use the following procedure to remove and replace the blower module.

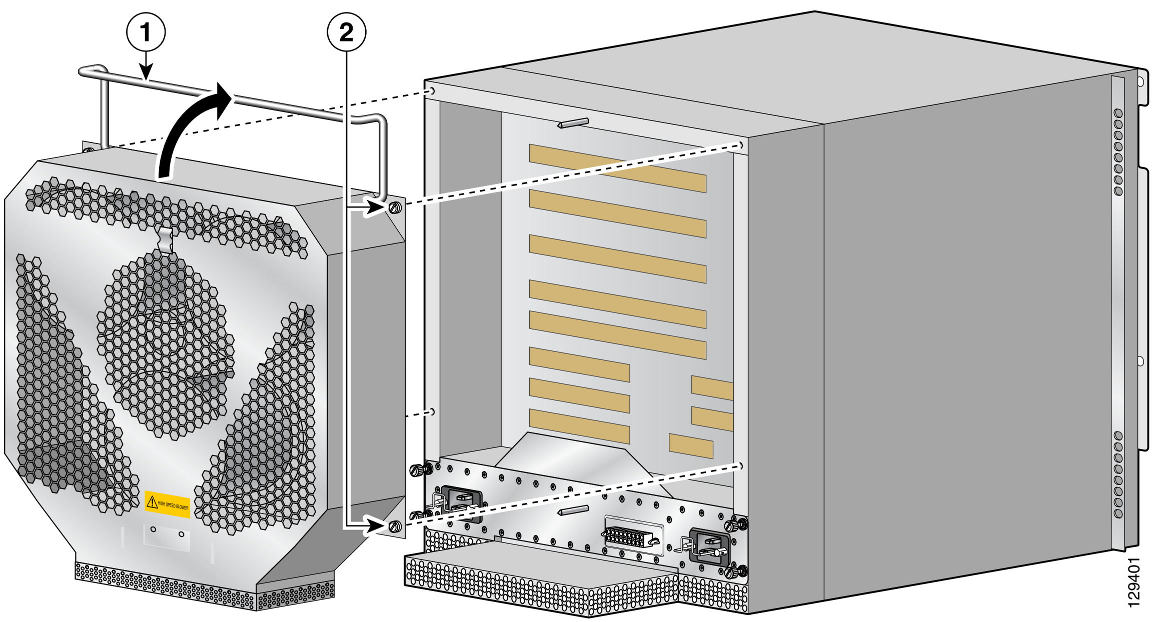
Step 1 Remove the blower module from the chassis (Figure 6-5):

a. Lift the blower module handle to its carrying position.

b. Loosen the four captive screws on the blower module faceplate.

c. Remove the blower module by grasping it on each side and pulling it straight back from the chassis.

Figure 6-5 Removing the Blower Module



1	Carrying handle	**2**	Captive screws (2 on each side)

Step 2 Install the new blower module (Figure 6-6):

a. Position the alignment holes on the blower module with the guide pins at the top of the chassis and on the PDU at the bottom of the chassis.

b. Slide the blower toward the chassis until it mates with the backplane connector.

Caution Electrical and control line connections for the blower module and backplane occur automatically when the connectors on the blower module and PDU mate. To prevent damage to the blower module and PDU connectors, do not use excessive force when installing the blower module against the rear of the chassis.

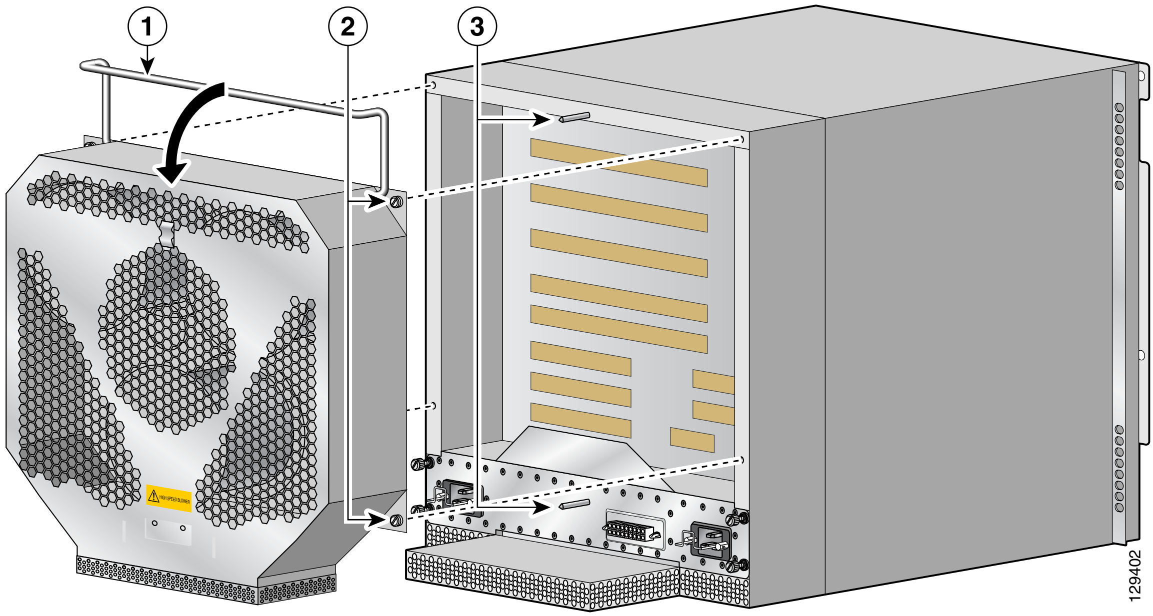
---

c. Tighten the four captive screws to secure the blower module to the chassis.

The (green) OK indicator should light. If the OK indicator does not light, see the "Troubleshooting the Blower Installation" section on page 6-12.

d. Lower the blower module handle to its operating position.

Figure 6-6 Installing the Blower Module



1	Carrying handle	**3**	Guide pins
2	Captive screws (2 on each side)		

Troubleshooting the Blower Installation

Use the following procedure to troubleshoot the blower module if it is not operating properly after installation.

Step 1 Be sure the router is powered on and that all power cords are connected properly.

Step 2 Loosen the four captive screws and reseat the blower module to the chassis. Retighten the captive screws to ensure the blower module is properly seated to the backplane connector.

Step 3 Check the blower module status indicators:

- OK (green)—This indicator should light as soon as the blower module is installed and receives power from the backplane connector. It indicates that the blower module is operating normally.
- Fail (red)—This indicator remains off during normal operation. If the indicator is on, the system has detected a fan failure or other fault in the blower module.
  - If this indicator remains on and the blower module fans fail to operate normally after several attempts to reseat the blower module, replace the existing blower module with a spare.
  - If the spare blower module also fails, power off the router and contact a Cisco service representative for assistance.

Removing and Replacing AC and DC Power Subsystem Components

This section contains removal and replacement procedures for the AC and DC power systems used with the Cisco 12006 and Cisco 12406 series routers. If you ordered an upgrade kit, you can use these same procedures to upgrade all of the power system components.

The illustrations in this procedure represent both original and upgraded power supplies and PDUs shipping with the Cisco 12006 and Cisco 12406 series routers. Depending on your system, these components may not look *exactly* like those in your chassis, but the removal and replacement procedures are essentially the same. Multiple illustrations are presented to represent original and new models where appropriate.

The following tools and equipment are required to remove and install power equipment:

- Number 1 Phillips screwdriver
- 3/16-inch flat-blade screwdriver
- An ESD-preventive wrist strap

Installation Guidelines

The Cisco 12006 and Cisco 12406 series routers support online insertion and removal (OIR). If you are replacing a redundant power supply, you can remove and install the power supply while the system remains powered on without causing an electrical hazard or damage to the system. This feature enables you replace a power supply while the system maintains all routing information and ensures session preservation.

However, to maintain operational redundancy, proper cooling, and meet EMI compliance standards, you must have both working power supplies installed. When you remove a failed power supply with the router in operation, perform the replacement as quickly as possible. Make sure you have the tools and the replacement power supply ready before beginning the removal and installation procedure.

Power Supply and PDU Compatibility

Cisco 12006 and Cisco 12406 series routers are available with either an AC or DC power supply system. The two types of power supplies for these systems are:

- Original power supplies (rated at 1400 watts) that shipped with earlier systems
- Enhanced capacity power supplies (rated at 1900 watts) that ship with current systems and upgrade kits

Removal and replacement procedures are the same for either type of power supply, but because of their power capacity and physical differences, you cannot mix different types of power supplies in the chassis.

Caution Newer, 1900 W DC power supplies require the upgraded PDU. You cannot install a new power supply using the old PDU. If you are replacing an old power supply with the new unit, you must perform a complete upgrade by replacing both power supplies, the PDU, *and the blower module* if you are required to meet NEBS extended temperature range requirements. This also means that you must shut down the router to perform the upgrade. Notify the system administrator and other appropriate personnel that all routing traffic stops while the upgrade takes place.

Before you attempt to install or replace them (Table 6-1Table 6-1), be sure you know your system power supplies and associated PDU.

Table 6-1 Original and Replacement Components

Original Component	Replacement Component
AC Power Distribution Unit (PDU) (GSR6-AC-PDU=) Compatible only with 1400 W power supplies.	**AC PDU (12000/6-AC-PDU=)** Required for 1900 W power supplies.
AC Power Supply (PWR-GSR6-AC=) Used to replace 1400 W power supplies only. All power supplies must be 1400 W. Do not mix with 1900 W power supplies.	**AC Power Supply (12000/6-AC-PEM=)** Used to replace existing power supplies. All power supplies must be 1900 W. Do not mix with 1400 W power supplies. If you are upgrading 1400 W power supplies to 1900 W power supplies, you must also upgrade to the new AC PDU (12000/6-AC-PDU=). **Caution** Redundancy in 1400 W power systems was not a requirement and used a blank filler (MAS-GSR-PWRBLANK=) in place of a second power supply to ensure EMI compliance. Newer 1900 W power supplies require redundancy. You must install two power supplies.

Table 6-1 Original and Replacement Components (Continued)

Original Component	Replacement Component
DC Power Supply (PWR-GSR6-DC=) Used to replace 1400 W power supplies only. Do not mix with 1900 W power supplies.	**DC Power Supply (12000/6-DC-PEM=)** Used to replace existing power supplies. All power supplies must be 1900 W. Do not mix with 1400 W power supplies. If you are upgrading 1400 W power supplies to newer 1900 W power supplies, you must also upgrade to the new DC PDU (12000/6-DC-PDU=) **Caution** Redundancy in 1400 W power systems was not a requirement and a blank filler (MAS-GSR-PWRBLANK=) was used in place of a second power supply to ensure EMI compliance. New 1900 W power supplies require redundancy...you must install two power supplies.
DC PDU (GSR6-DC-PDU=) Compatible only with 1400 W power supplies.	**DC PDU (12000/6-DC-PDU=)** Required for 1900 W power supplies.

Installing Upgrade Kits

When installing a power system upgrade kit, replace the following components.

- AC power upgrade (12000/6-AC-UP=):
  - Power supplies (Removing and Replacing an AC PEM, page 6-18)
  - PDU (Removing and Replacing an AC PDU, page 6-24)
- DC power upgrade (12000/6-DC-UP=):
  - Power supplies (Removing and Replacing a DC PEM, page 6-31)
  - PDU (Removing and Replacing a DC PDU, page 6-37)

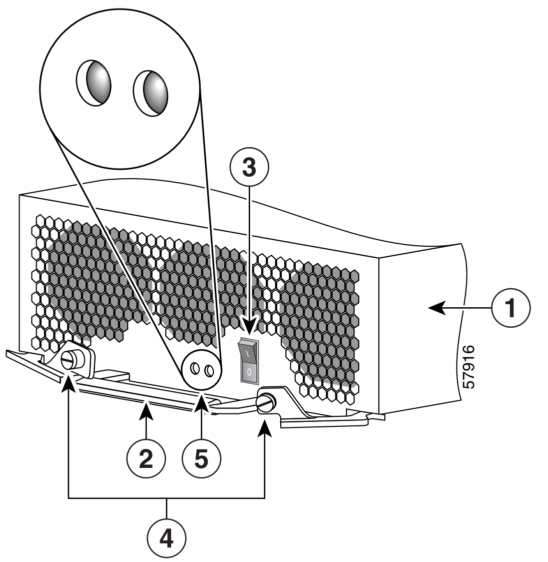
Note A blower upgrade (not included in the power upgrade kit) is also required to meet NEBS extended temperature range requirements. To order the blower upgrade (12000/6-BLOWER=), contact your Cisco representative.

Removing and Replacing an AC PEM

This section contains the procedure to remove and replace an AC PEM from the chassis. *Before* you begin this procedure, be sure to read the "Installation Guidelines" section on page 6-14.

Figure 6-7 identifies the components of an AC power supply.

Figure 6-7 AC Power Supply Components



1	AC PEM	**4**	Captive screws/release levers
2	Handle	**5**	AC input/DC output status indicators
3	Power On/Off switch		

Use the following procedure to remove and replace an AC power supply.

Caution You cannot mix power supply types within the chassis. If you are replacing a 1400 W power supply from an older system with a new 1900 W power supply, you must replace both power supplies, the AC PDU, *and the blower module* if you are required to meet NEBS extended temperature range requirements (see the "Power Supply and PDU Compatibility" section on page 6-14 for additional information). You must shut down the router to perform the upgrade. Notify the system administrator and other appropriate personnel that all routing traffic stops while upgrades take place.

Step 1 Set the power switch to the Off (0) position.

Step 2 Unplug the power supply cord from its AC outlet.

Step 3 Power off the circuit breaker assigned to that AC outlet.

Step 4 Remove the PEM from the chassis (Figure 6-8):

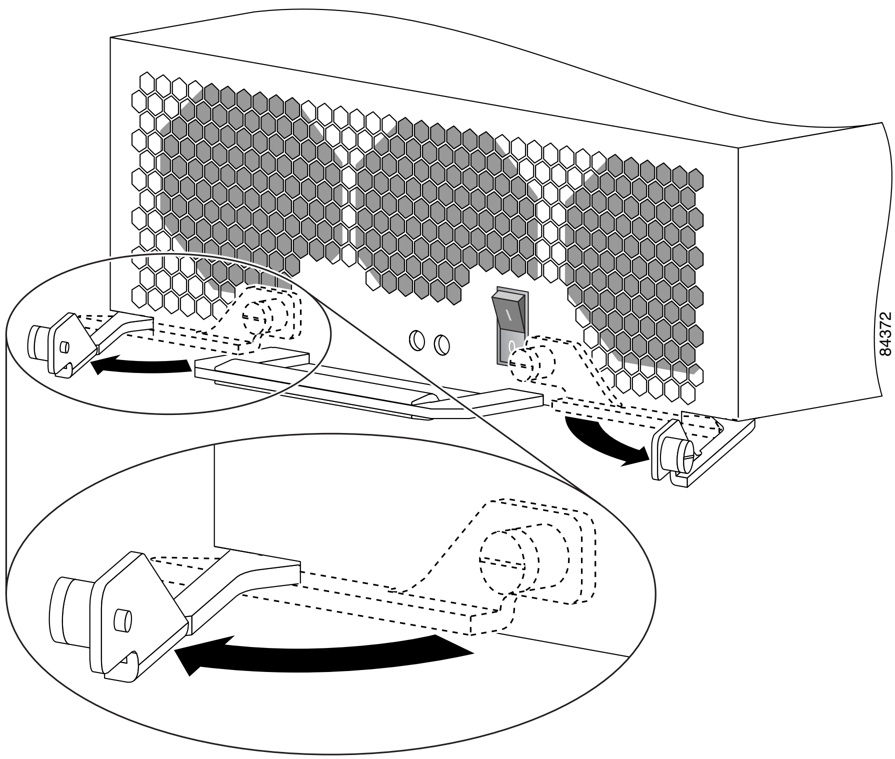
a. Loosen the captive screw on each ejector lever.

b. Pivot open the levers to eject the power supply.

c. Slide the power supply out of its bay while supporting it with your other hand.

Warning **The power supply weighs approximately 14 lb (6.35 kg). Use two hands to remove the power supply.**

Figure 6-8 Releasing the AC Power Supply



Step 5 Install the new power supply (Figure 6-9):

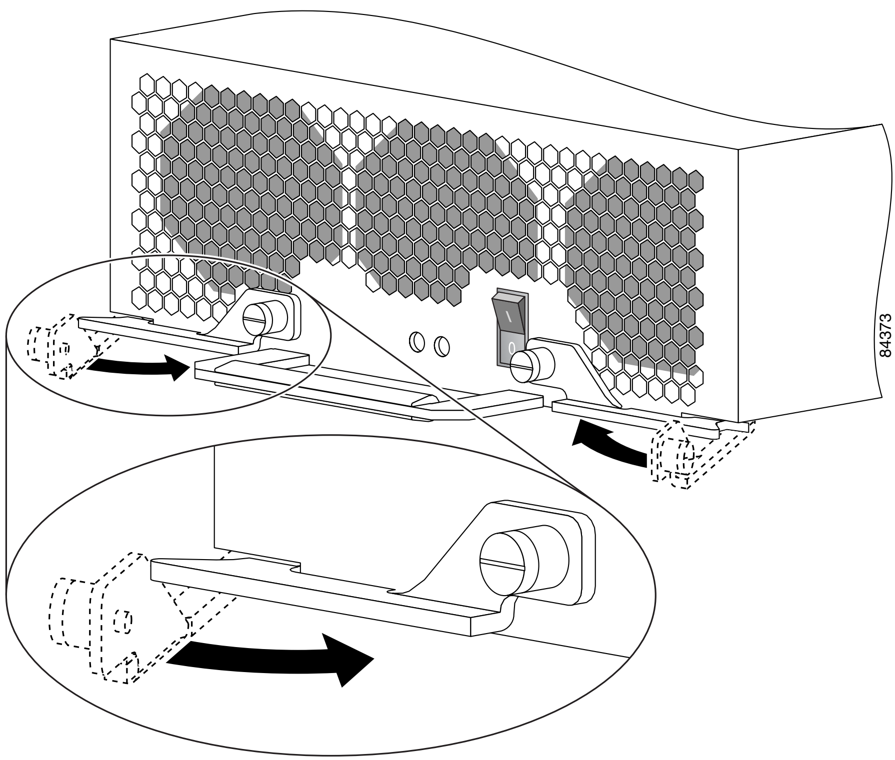
a. Slide the power supply into the bay until it mates with its backplane connector.

Caution To prevent damage to the power shelf backplane connector, do not use excessive force when inserting the power supply into the chassis.

---

b. Close the ejector levers and tighten the captive screws to securely seat the power supply to the backplane connector.

Figure 6-9 Seating the AC Power Supply



Step 6 Plug the power supply cable into its AC outlet.

Step 7 Power on the circuit breaker to that AC outlet.

Step 8 Set the power switch to the On (1) position.

The AC Input and DC Output power indicators on the front of the power supply should light. If the indicators do not light, see the "Troubleshooting the AC Power Supply Installation" section on page 6-22.

Troubleshooting the AC Power Supply Installation

Use the following procedure to troubleshoot the AC power supply if it is not operating properly after installation.

Step 1 Make sure the power supply is seated properly:

- Eject and reseat the power supply. Make sure:
  - The captive screws on the ejector levers are tightened securely.
  - The power switch is set to the On (1) position.

Step 2 Make sure the router is powered on and that all power cords are connected properly:

- Power cords on the back of the chassis are secured to the PDU with their retention clips.
- Power cords at the power source end are connected to a dedicated AC power outlet.
  - Each AC power supply operating in the nominal range of 200 to 240 VAC requires a minimum service of 20A, North America (or 16A, international).
- Make sure the source AC circuit breaker is switched on.

Step 3 Check the power supply status indicators:

- AC Input (green)—Indicates that the power supply is operating normally, and the source AC voltage is within the nominal operating range of 200 VAC to 240 VAC. This indicator lights when the power supply switch is set to the On (1) position.
  - If the AC Input power indicator remains off after checking all of the power sources, replace the power supply with a spare.
  - If the spare power supply does not work, replace the PDU.
- DC Output (green)—Indicates that the power supply is operating normally, and the output DC voltage is within the nominal operating range of –48 VDC to –60 VDC. This indicator lights when the power switch is set to the On (1) position.

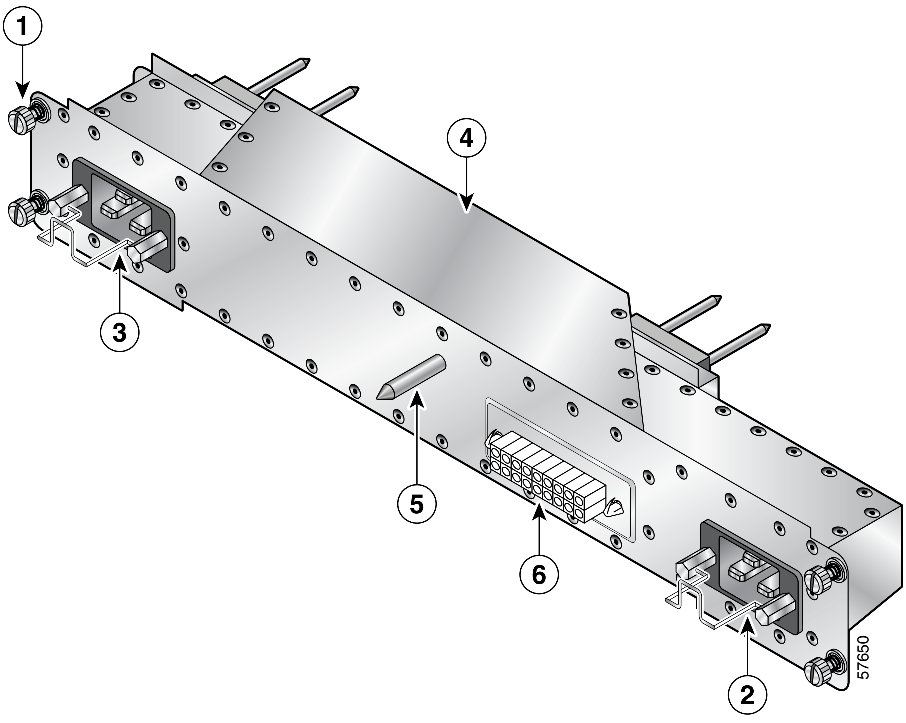
  If the indicator is off, toggle the power switch off and then on. If the indicator remains off after several attempts to power it on, replace the power supply with a spare.

Removing and Replacing an AC PDU

Use the following procedure to remove and replace an AC PDU. *Before* you begin this procedure, read the "Installation Guidelines" section on page 6-14.

Figure 6-10 identifies the components of the AC PDU.

Figure 6-10 AC Power Distribution Unit



1	Captive screw	**4**	AC power distribution unit
2	AC power cord connector/retention clip (A)	**5**	Guide pin
3	AC power cord connector/retention clip (B)	**6**	Blower module connector

Caution The system must be powered off to remove and replace the PDU. Notify the network administrator and other appropriate personnel that all routing traffic stops while replacements take place.

Step 1 Power off both power supplies by setting the power switches to the Off (0) position.

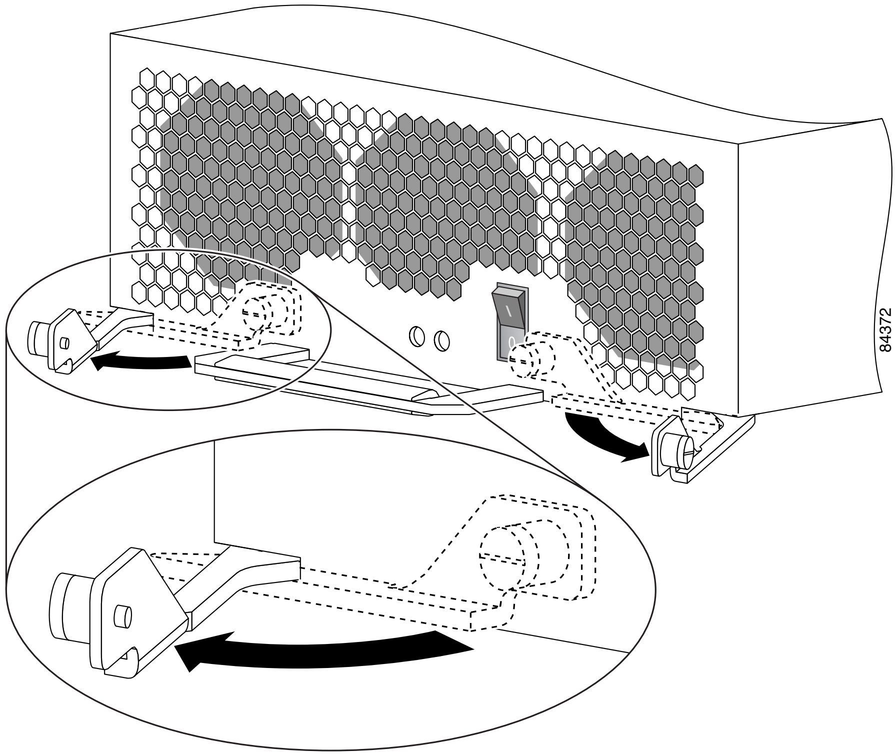
Step 2 Unplug the power supply cords from their AC outlets.

Step 3 Power off the circuit breakers assigned to the AC outlets.

Step 4 Loosen the captive screw on each ejector lever and pivot the levers open to unseat the power supply from its PDU connector (Figure 6-11).

- It is not necessary to remove the power supply from its bay.
- Repeat this step for the second power supply.

Figure 6-11 Unseating the AC Power Supply

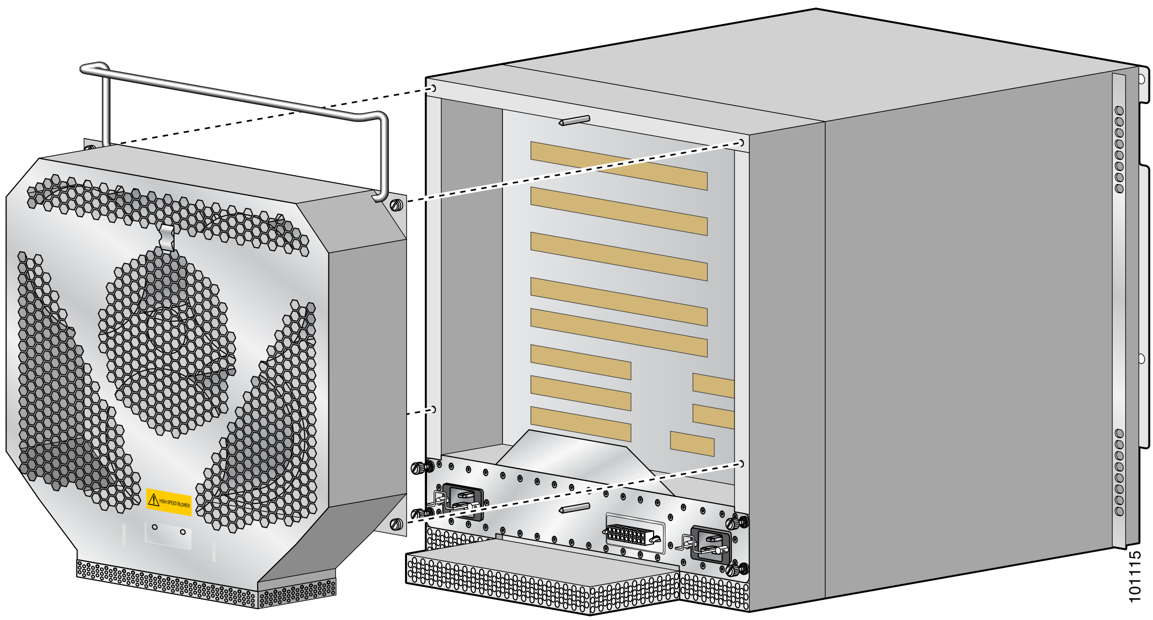


Step 5 Release the retention clip and disconnect each power supply cord from the PDU (see Figure 6-10).

Step 6 Remove the blower module (Figure 6-12):

- **a.** Lift the blower module handle to its raised (carrying) position.
- **b.** Loosen the (4) captive screws on the blower module.
- **c.** Remove the blower module by grasping it on each side and pulling it straight back from the chassis.

Figure 6-12 Removing the Blower Module



Step 7 Remove the PDU from the chassis (Figure 6-13):

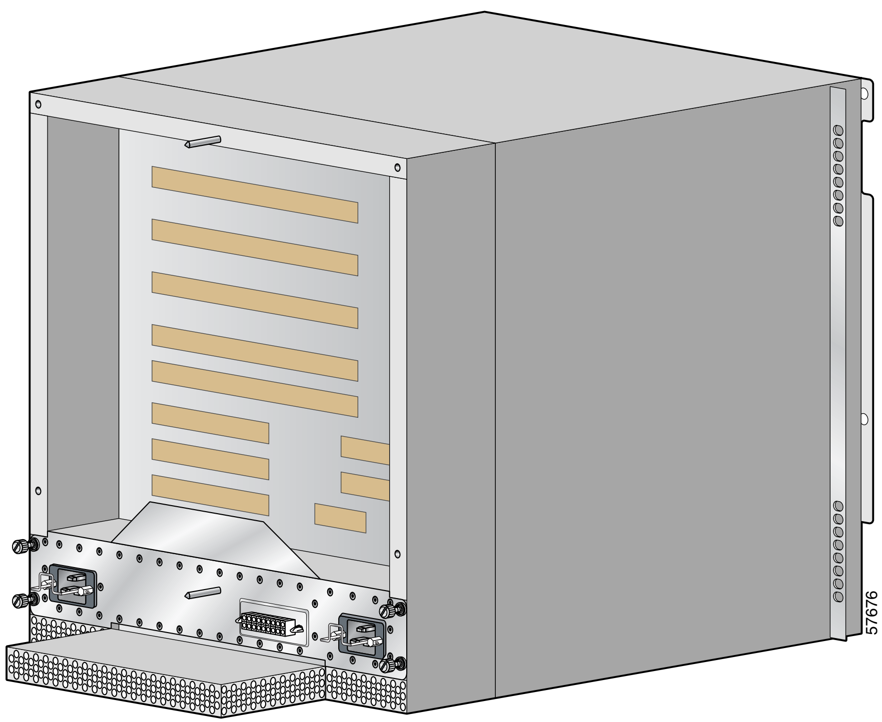
a. Loosen the (4) captive screws on the PDU.

b. Grasp the PDU and pull it out slightly.

c. Move the PDU to the left and pivot the right side through the opening to remove the PDU from the chassis opening.

> **Note** Tilting the PDU at a slight angle makes it easier to remove it from the chassis.

Figure 6-13 Removing the AC PDU



Step 8 Install the new PDU and tighten its (4) captive screws to secure it to the chassis.

Step 9 Install the blower module (Figure 6-14):

a. Position the alignment holes on the blower module with the guide pins on the chassis and PDU.

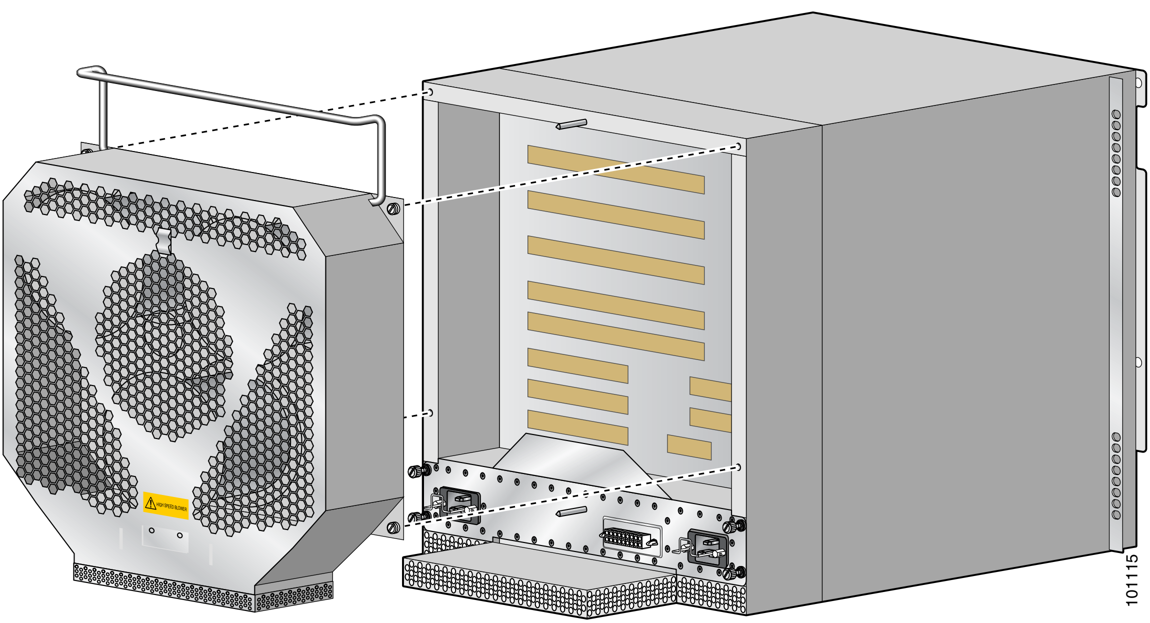
b. Slide the blower over the guide pins toward the chassis until it mates with the PDU connector.

Caution To prevent damage to the connectors, do not use excessive force when installing the blower module.

c. Tighten the (4) captive screws to secure the blower module to the chassis.

d. Lower the carrying handle to its operating position.

Figure 6-14 Installing the Blower Module



Step 10 Reconnect the power cords to the PDU and secure them using their retention clips.

Step 11 Plug the power cords into their AC outlets.

Step 12 Power on the circuit breakers assigned to the AC outlets.

Step 13 Reinstall the power supplies (Figure 6-15):

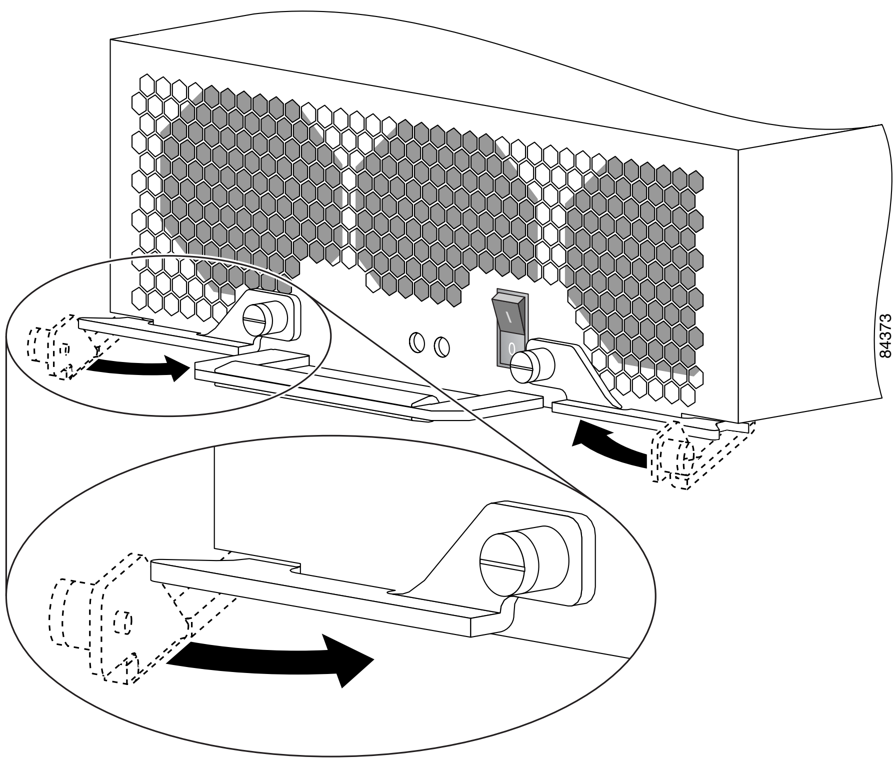
a. Push the power supply into its bay until it mates with its PDU connector.

Caution To prevent damage to the connectors, do not use excessive force when inserting the power supply into the chassis.

b. Close the ejector levers and tighten the captive screws to securely seat the power supply to the chassis.

c. Repeat steps **a.** and **b.** for the second power supply.

Figure 6-15 Seating the AC Power Supply



Step 14 Set the power switch on both power supplies to the On (1) position.

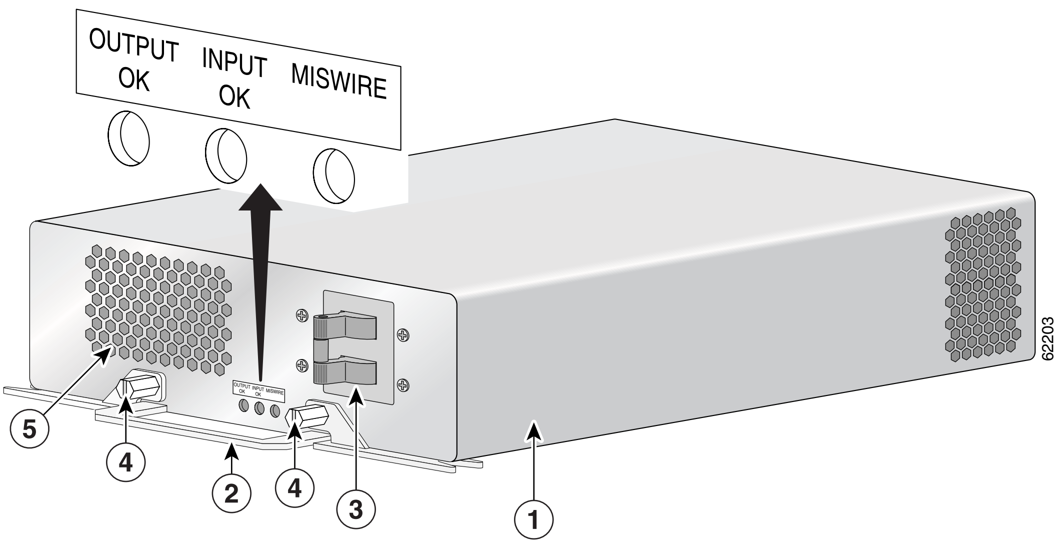
The AC Input Power and DC Output Power indicators on the power supplies should light. If the indicators do not light, see the "Troubleshooting the AC Power Supply Installation" section on page 6-22.

Removing and Replacing a DC PEM

This section contains the procedure to remove and replace a DC power supply from the chassis. *Before* you begin this procedure, read the "Installation Guidelines" section on page 6-14.

Figure 6-16 identifies the components of a DC power supply.

Figure 6-16 DC Power Entry Module Components



1	DC PEM	**4**	Captive screws/release levers
2	Handle	**5**	Cooling fan
3	Power On/Off switch	**6**	AC input/DC output/miswire status indicators

Use the following procedure to remove and replace a DC power supply.

Caution You cannot mix power supply types within the chassis. If you are replacing a 1400 W power supply with a 1900 W power supply, you must replace both power supplies, the DC PDU, *and the blower module* if you are required to meet NEBS extended temperature range requirements (see the "Power Supply and PDU Compatibility" section on page 6-14 for additional information). You must shut down the router to perform the upgrade. Notify the system administrator and other appropriate personnel that all routing traffic will stop while the upgrade takes place.

Step 1 Set the power switch to the Off position.

Step 2 Power off the circuit breaker assigned to the power supply.

Warning **To ensure that power remains off while you are performing this procedure, tape the circuit breaker switch in the Off (0) position.**

Step 3 Remove the power supply from the chassis (Figure 6-17):

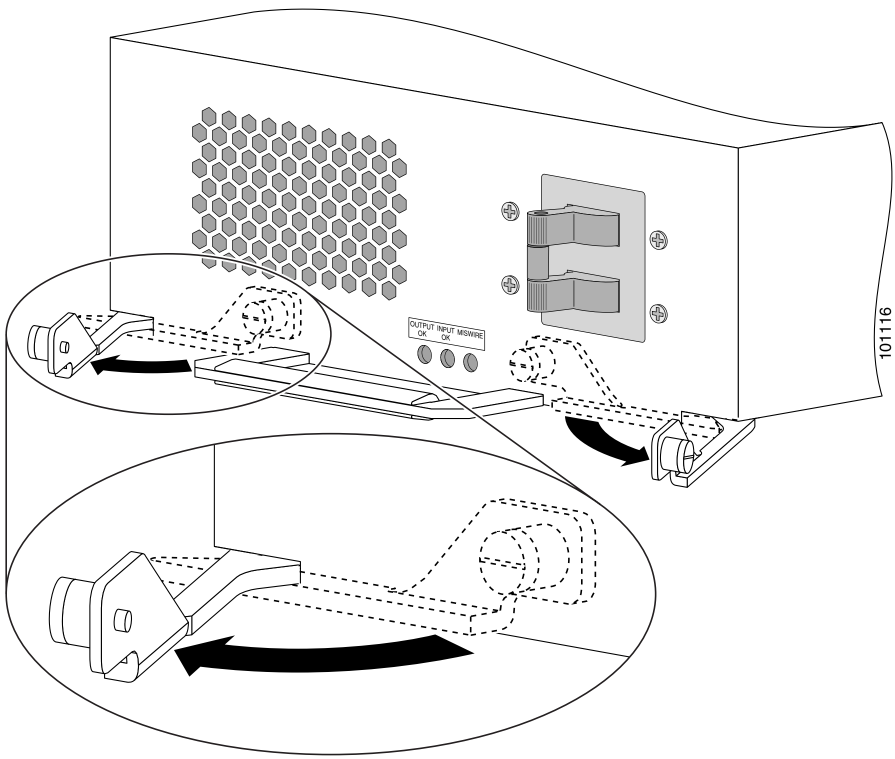
a. Loosen the captive screw on each ejector lever.

b. Pivot the levers open to release the power supply from its bay.

c. Slide the power supply out of its bay while supporting it with your other hand.

Warning **The power supply weighs approximately 10 lb (4.5 kg). Use two hands to remove the power supply.**

Figure 6-17 Releasing the DC Power Supply



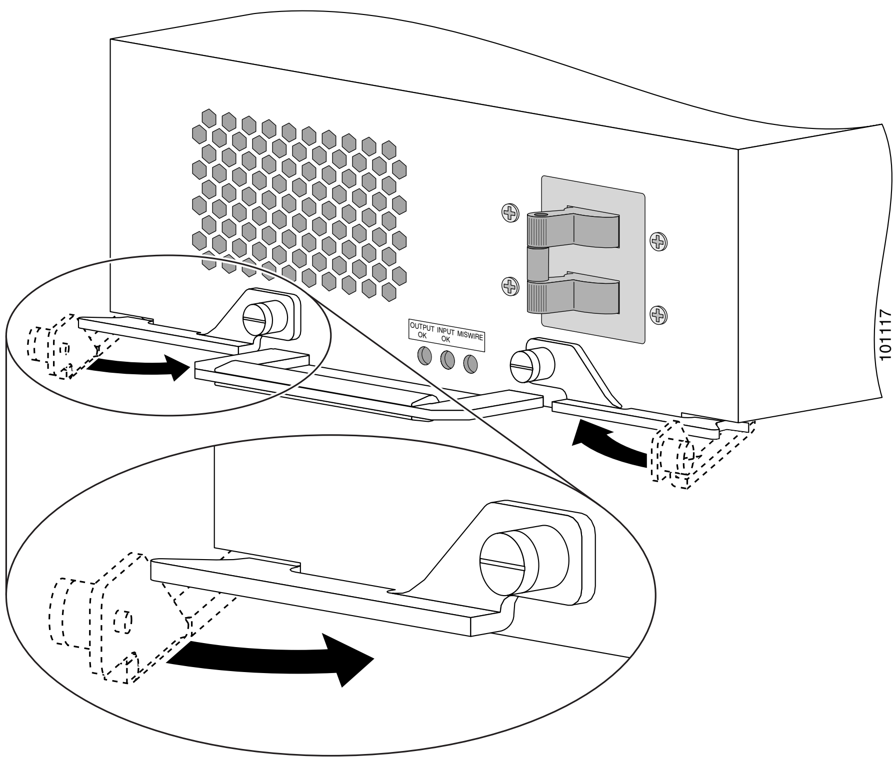
Step 4 Install the new power supply:

a. Slide the power supply into the bay until it mates with its backplane connector.

Caution To prevent damage to the power shelf backplane connector, do not use excessive force when inserting the power supply into the chassis.

b. Close the ejector levers and tighten the captive screws to securely seat the power supply to the backplane connector (Figure 6-18).

Figure 6-18 Seating the DC Power Supply



Step 5 Power on the circuit breaker.

Step 6 Set the power switch to the On position.

The AC Input and DC Output power indicators on the front of the power supply should light. If the indicators do not light, or the Miswire indicator is on, see the "Troubleshooting the DC Power Supply Installation" section on page 6-35.

Troubleshooting the DC Power Supply Installation

Use the following procedure to troubleshoot the DC power supply if it is not operating properly after installation.

Step 1 Make sure the power supply is seated properly:

- Eject and reseat the power supply.
  - The captive screw on the ejector lever are tightened securely.
  - The power switch is set to the On (1) position.

Step 2 Make sure the router is powered on and that all power cables are connected properly:

- Power leads are securely connected to the power connector block on the PDU.
- Power cables are securely connected at the DC source connection.
- The source DC circuit breaker is turned on.

Step 3 Check the power supply status indicators:

- Output OK (green)—Indicates that the PEM is operating normally, and the source DC output voltage is within the nominal operating range of –48 to –60 VDC. This indicator should light when the power switch is set to the On (1) position.

  If the indicator is off, toggle the power switch off and then on. If the indicator remains off after several attempts to power it on, replace the power supply with a spare.

- Input OK (green)—Indicates that the power supply is operating normally, and the source DC input voltage is within the nominal operating range of -40.5VDC to -75VDC. This indicator should light when the power supply switch is set to the On (1) position.
  - If the Input OK indicator remains off after checking all of the power sources, replace the power supply with a spare.
  - If the spare power supply does not work, replace the PDU.
- Miswire (amber)—Indicates the input wiring is incorrect at the PDU power connection block.

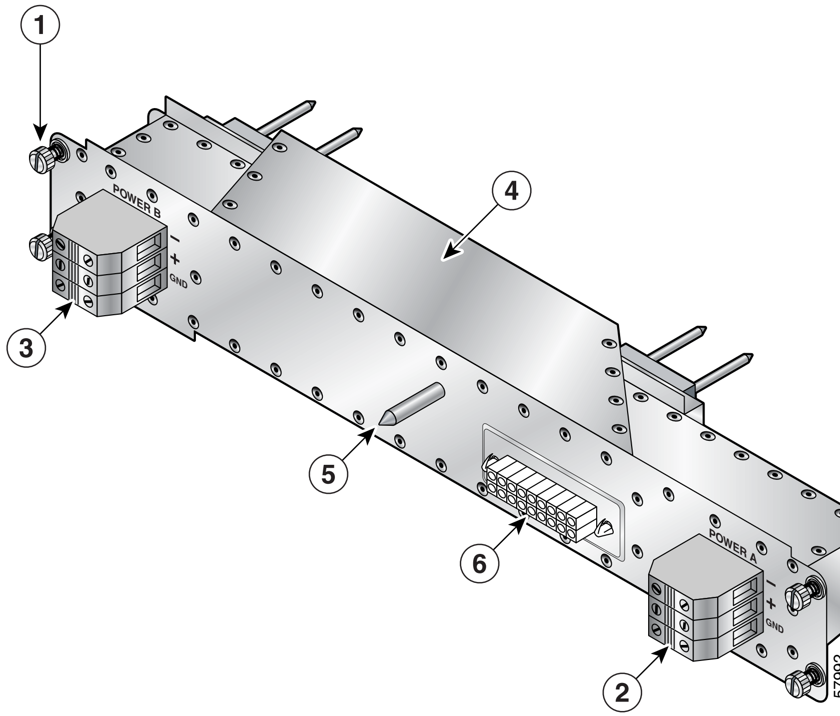
  Correct wiring to the DC power connector block (see Figure 6-25).

Removing and Replacing a DC PDU

Use the following procedure to remove and replace a DC PDU. *before* beginning this procedure, read the "Installation Guidelines" section on page 6-14.

Figure 6-19 identifies the components of the DC PDU.

Figure 6-19 DC Power Distribution Unit



1	Captive screw	**4**	DC power distribution unit
2	DC power connector block (A)	**5**	Guide pin
3	DC power connector block (B)	**6**	Blower module connector

Caution The system must be powered off to remove and replace the PDU. Notify the network administrator and other appropriate personnel that all routing traffic will stop while the replacement takes place.

Step 1 Power off both power supplies by setting their power switches to the Off (0) position (see Figure 6-16).

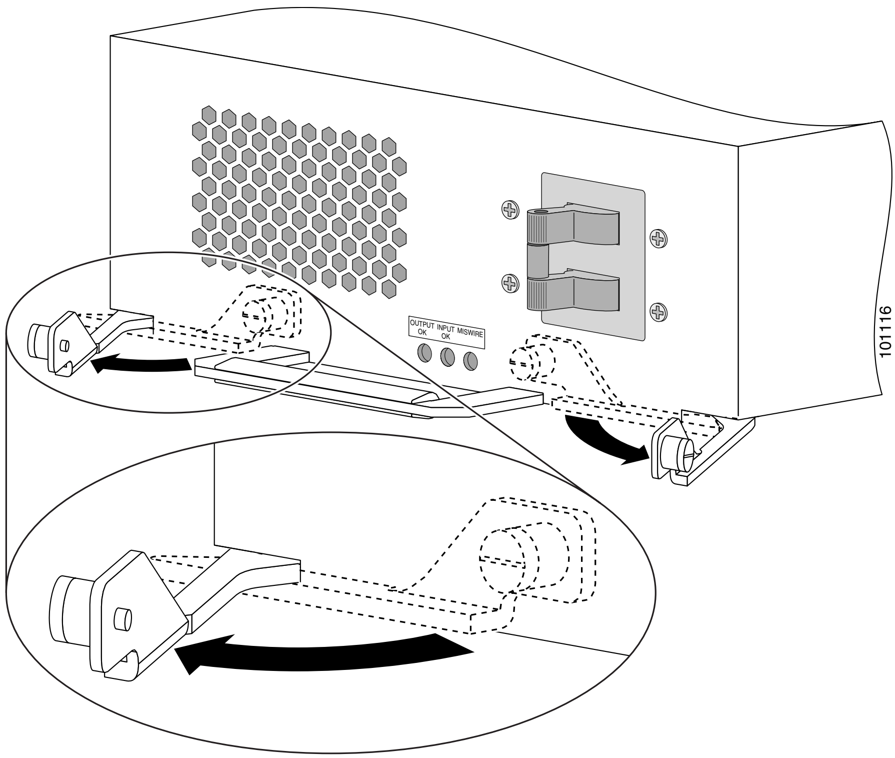
Step 2 Power off the circuit breakers assigned to the power supplies.

Warning **To ensure that power remains off while you are performing this procedure, tape the circuit breaker switches in the Off (0) position.**

Step 3 Loosen the captive screw on each ejector lever and pivot the levers open to unseat the power supply from its PDU connector (Figure 6-20).

- It is not necessary to remove the power supply from its bay.
- Repeat this step for the second power supply.

Figure 6-20 Unseating the DC Power Supply



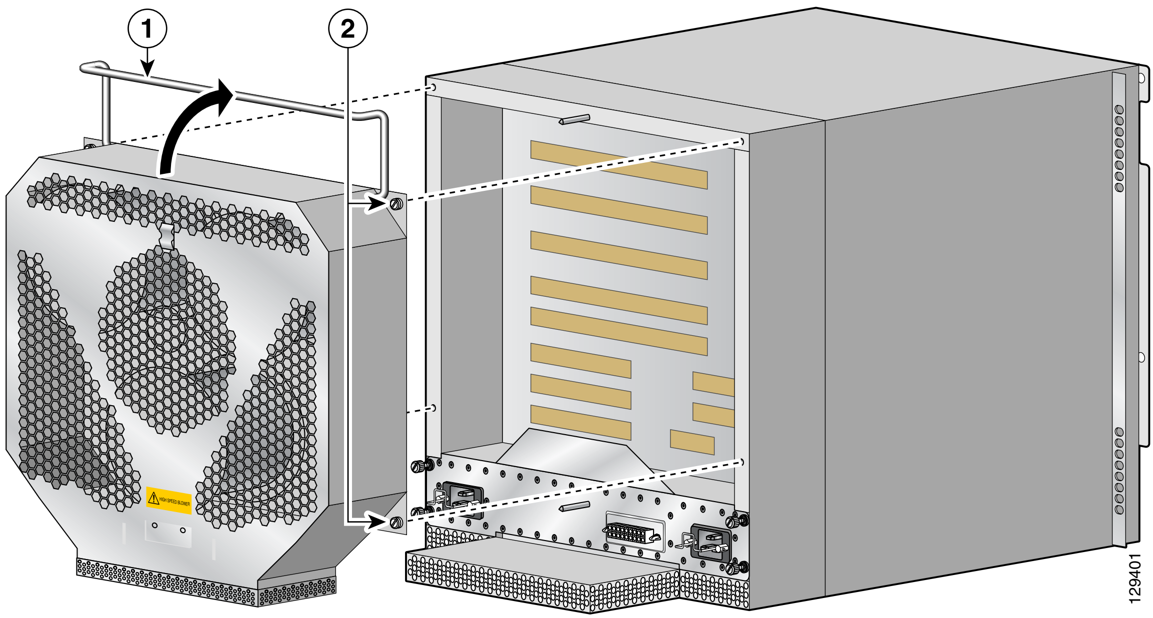
Step 4 Remove the blower module (Figure 6-21):

   a. Lift the blower module handle to its raised (carrying) position.

   b. Loosen the (4) captive screws on the blower module.

   c. Remove the blower module by grasping it on each side and pulling it straight back from the chassis.

Figure 6-21 Removing the Blower Module



Step 5 Disconnect the DC power leads from the PDU power connector blocks in the following order (Figure 6-22):

a. Negative lead from the top port.

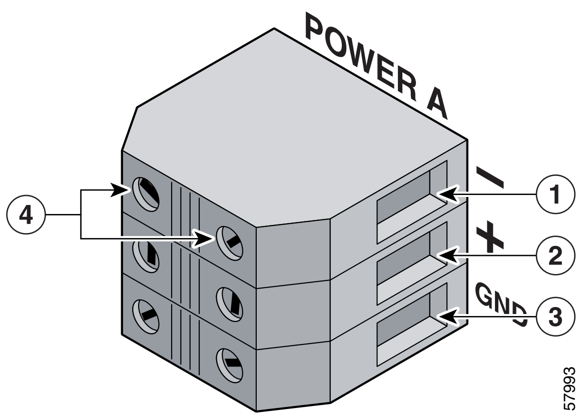
b. Positive lead from the middle port.

c. Ground lead from the bottom port.

d. Repeat these steps for the second power connector block.

Warning **To prevent injury and damage to the equipment, always remove the source DC power leads and ground from the power shelf terminals in the following order: (a) negative (–), (b) positive (+), (c) ground.**

Figure 6-22 Disconnecting the DC Power Leads



1	Negative terminal port	**3**	Ground terminal port
2	Positive terminal port	**4**	Terminal port connector screws

Step 6 Remove the PDU from the chassis (Figure 6-23):

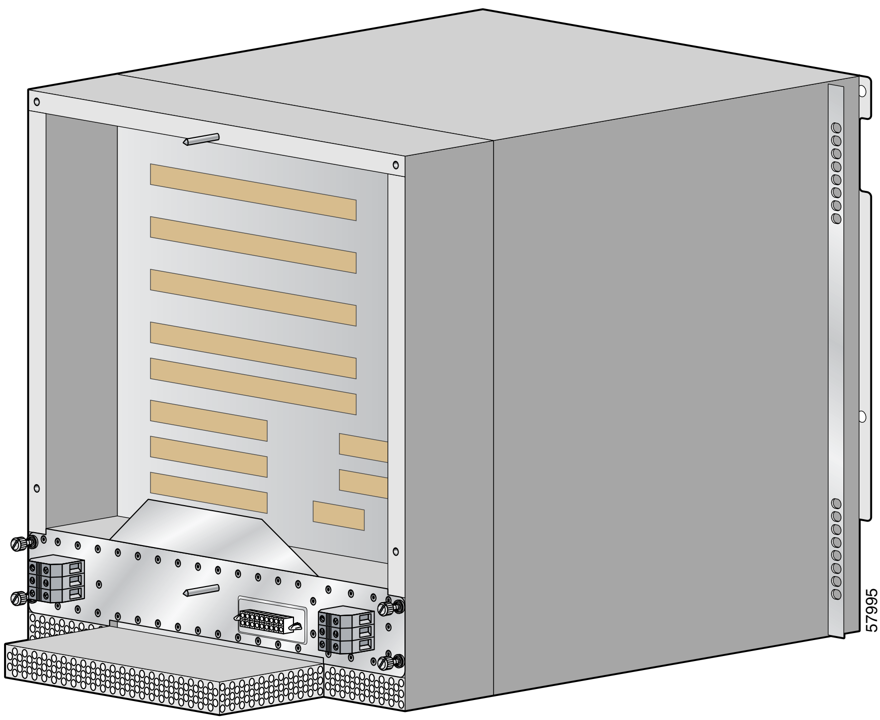
a. Loosen the (4) captive screws on the PDU.

b. Grasp the PDU and pull it out slightly.

c. Move the PDU to the left and pivot the right side through the opening to remove the PDU from the chassis.

Note Tilting the PDU at a slight angle makes it easier to remove it from the chassis.

Figure 6-23 Removing the DC PDU



Step 7 Install the new PDU and tighten its (4) captive screws to secure it to the chassis.

Step 8 Install the blower module (Figure 6-24):

a. Position the alignment holes on the blower module with the guide pins on the chassis and PDU.

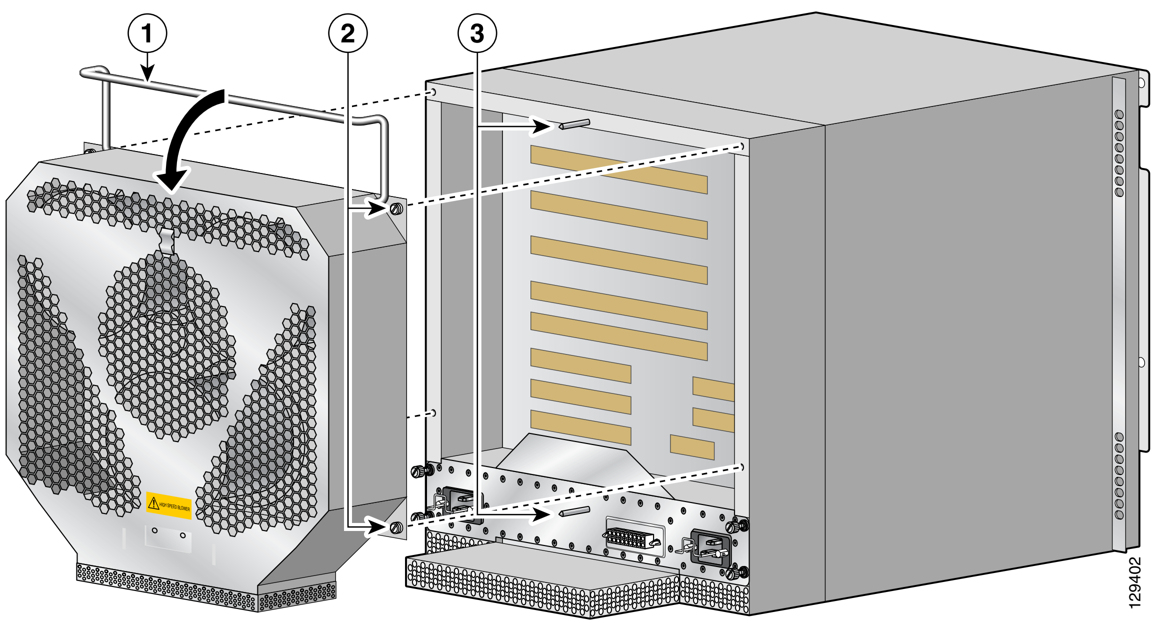
b. Slide the blower over the guide pins toward the chassis until it mates with the backplane connector.

Caution To prevent damage to the connectors, do not use excessive force when installing the blower module.

c. Tighten the (4) captive screws to secure the blower module to the chassis.

d. Lower the carrying handle to its operating position.

Figure 6-24 Installing the Blower Module



Step 9 Reconnect the DC power leads to the PDU power connector blocks in the following order (Figure 6-25):

a. Ground lead to the bottom port.

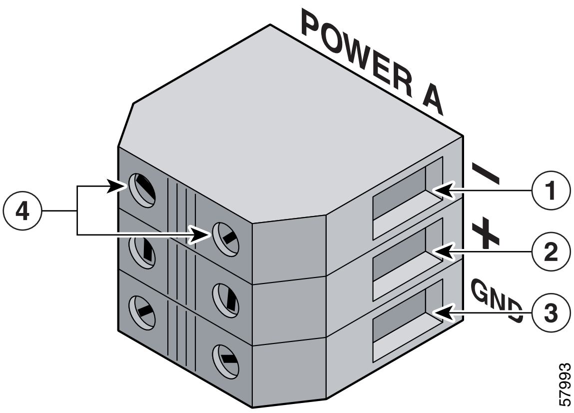
b. Positive lead to the middle port.

c. Negative lead to the top port.

d. Repeat these steps for the second power connector block.

Warning **To prevent injury and damage to the equipment, always attach the ground and source DC power leads to the power block connector in the following order: (a) ground to ground, (b) positive (+) to positive (+), (c) negative (–) to negative (–).**

Figure 6-25 Disconnecting the DC Power Leads



1	Negative terminal port	**3**	Ground terminal port
2	Positive terminal port	**4**	Terminal port connector screws

Step 10 Power on the circuit breakers assigned to the power supplies.

Step 11 Reinstall the power supplies:

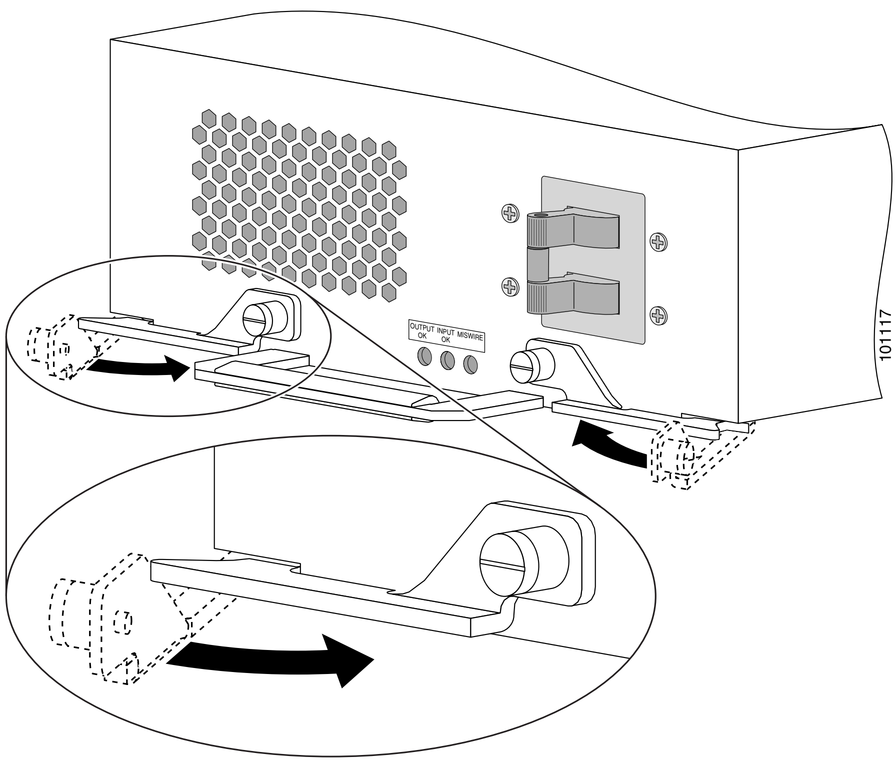
a. Push the power supply into its bay until it mates with its PDU connector.

> **Caution** To prevent damage to the connectors, do not use excessive force when inserting the power supply into the chassis.

b. Close the ejector levers and tighten the captive screws to securely seat the power supply to the chassis (Figure 6-26).

c. Repeat steps **a.** and **b.** for the second power supply.

Figure 6-26 Seating a DC Power Supply



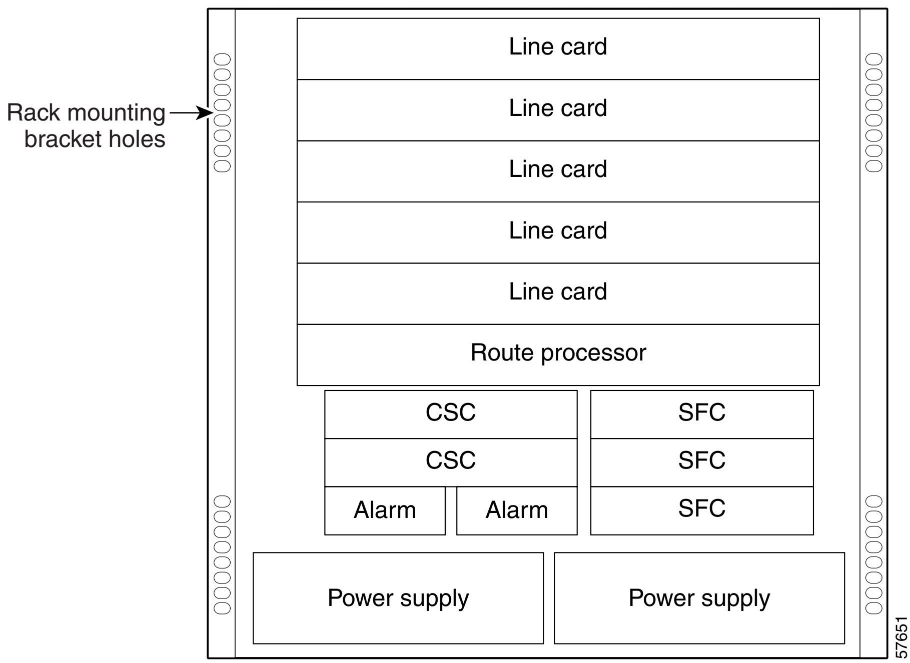
Step 12 Power on the power supplies.

The Output Power OK and Input Power OK indicators on the power supplies should light. If the indicators do not light, see the "Troubleshooting the DC Power Supply Installation" section on page 6-35.

Removing and Installing an RP or a Line Card

Line cards can occupy any slot, slot 0 (the top slot) through slot 4, in the RP and line card cage. (See Figure 6-27.) Your Cisco 12006 or Cisco 12406 Router is configured with the RP in slot 5 (the bottom slot). A redundant RP can be installed in any slot. The redundant RP requires a line card spacer to comply with EMI emission standards.

Figure 6-27 Cisco 12006 and Cisco 12406 routers Card Cage Slot Locations



Additional line card information can be found in the installation and configuration note for each type of line card. These notes accompany every line card that ships from the factory as an FRU.

Tools and Equipment

To remove and replace a line card, you need the following items:

- ESD-preventive strap
- 3/16-inch flat-blade screwdriver
- Replacement line card or RP

Removing an RP or Line Card

Cisco 12000 Series line cards support OIR, so they can be removed and installed while the router remains powered up. RPs also support OIR, but are hot-swappable only when the system is equipped with two RPs.

To remove an RP or line card from the RP and line card cage, see Figure 6-28 and follow these steps:

Step 1 Attach an ESD-preventive strap to your wrist and connect the leash to the chassis or to another grounded, bare metal surface.

Step 2 Identify the line card to be replaced and write down the following information:

- The slot number and type of line card
- The network interface cable connection ports on the line card

Step 3 On cards with multiple ports, start with the left port on the card and disconnect the interface cable connectors from each of the ports.

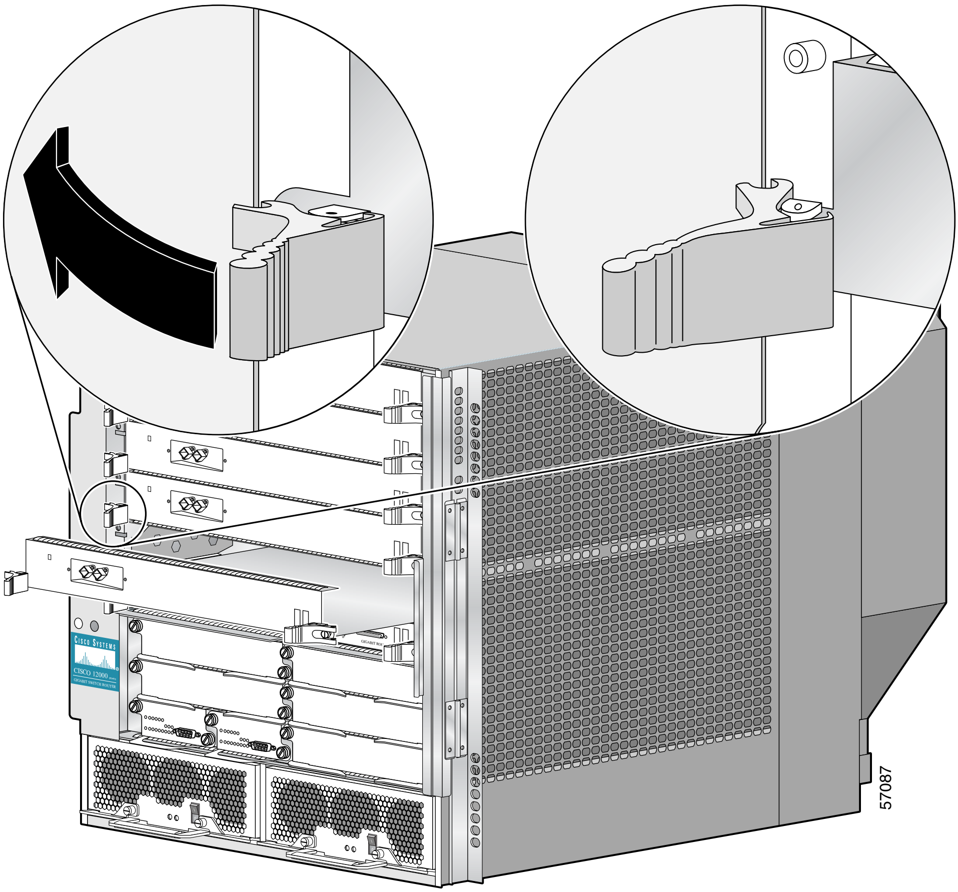
Step 4 After all the interface cables are disconnected, loosen the two captive screws on the cable-management bracket and pull the bracket away from the card.

Step 5 Loosen the two ejector lever captive screws at each end of the line card faceplate.

Step 6 Simultaneously pivot the ejector levers away from each other to unseat the line card from the backplane connector. Rotate each ejector lever outward away from the faceplate. (See Figure 6-28.)

Caution Fully remove each line card from its slot. Do not allow a line card to rest partially inserted into a slot, because that will damage the EMI shielding on the RP or line card in the slot directly below.

Figure 6-28 Removing an RP or Line Card from the Card Cage



Step 7 Grasp the edges of the line card carrier with both hands to support it, and fully remove the line card from the slot.

Caution One edge of the card carrier faceplate is lined with an EMI-preventive gasket consisting of many raised, conductive contacts. Be careful not to damage the gasket contacts, because a damaged card carrier gasket can reduce EMI performance.

Step 8 Immediately place the line card in an antistatic bag to protect it against ESD and to prevent dust from getting to the fiber-optic connectors on fiber-optic line cards.

Note If a line card slot in the card cage is not populated with a line card, a blank line card must be installed to avoid overheating and to ensure electromagnetic compliance (EMC).

If you plan to return the defective line card to the factory, repackage it in the shipping container you received with the replacement line card.

Installing an RP or Line Card

To install a line card in the RP and line card cage, follow these steps:

Step 1 Attach an ESD-preventive strap to your wrist and connect the leash to the chassis or to another grounded, bare metal surface.

Step 2 Check the slot assignment and network interface cable information that you wrote down before you removed the other RP or line card.

Caution Handle the RP or line cards by the metal card carrier edges only; avoid touching the board itself or any connector pins.

Step 3 Remove the RP or line card from its shipping package and antistatic bag.

Step 4 Set both edges of the RP or line card carrier into the card slot carrier alignment grooves on either side of the card cage.

Caution Do not allow a line card to rest partially inserted into a slot, because that will damage the EMI shielding on the RP or line card in the slot directly below.

Step 5 Pivot the ejector levers away from each other; rotate each ejector lever outward away from the faceplate.

Step 6 Grasp the edges of the metal card carrier with both hands to support and guide the RP or line card into the slot alignment grooves in the card cage.

Caution One edge of the card carrier faceplate is lined with an EMI-preventive gasket consisting of many raised, conductive contacts. Be careful not to damage the gasket contacts, because a damaged card carrier gasket can reduce EMI performance.

Step 7 Use both thumbs to slide the card carrier into the RP and line card slots until the ejector levers make contact with the front of the card cage, then *stop*.

Step 8 Grasp the two RP or line card ejector levers and pivot them toward the card faceplate until they are perpendicular to the faceplate, to seat the RP or line card in the backplane connector.

Step 9 Tighten the captive screws on each side of the card faceplate to prevent the RP or line card from becoming partially dislodged from the backplane and to ensure proper EMI shielding.

Note The line card captive screws must be tightened to meet EMI specification standards.

Repeat Step 2 through Step 9 for any additional replacement RPs or line cards, then proceed to the "Reconnecting Cables to a Line Card" section on page 6-54.

Adding an RP or Line Card

To install a new RP or line card in the RP and line card cage, follow these steps:

Step 1 Attach an ESD-preventive strap to your wrist and connect the leash to the chassis or to another grounded, bare metal surface.

Step 2 Identify the card slot for the new line card.

Step 3 Remove the blank faceplate covering the card slot.

Step 4 If installed, remove the narrow card filler panel at the top of the blank card slot.

Caution Handle line cards by the metal card carrier edges only; avoid touching the board itself or any connector pins.

Step 5 Go to Step 3 of the procedure "Installing an RP or Line Card" on page 6-50 to continue the installation of an RP or line card.

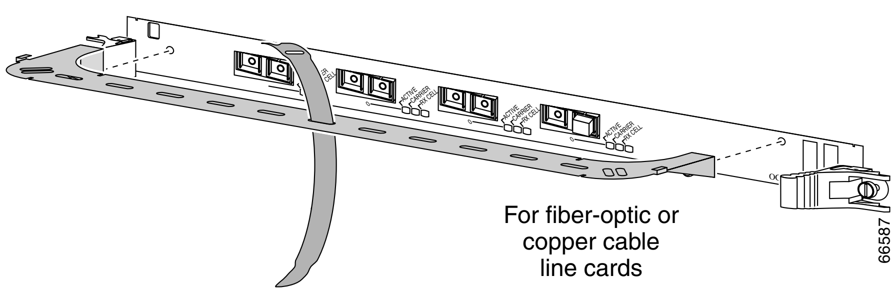
Step 6 Repeat Step 2 through Step 5 for any additional card installations.

Note If a line card slot in the card cage is not populated with a line card, a blank line card must be installed to avoid overheating and to ensure electromagnetic compliance (EMC).

Installing a Line Card Cable-Management Bracket

When you install a new line card, you must install the line card cable-management bracket on the faceplate of the line card before connecting cables to the ports. Figure 6-29 shows a typical line card cable-management bracket oriented and aligned for installation on a line card in a Cisco 12006 or Cisco 12406 Router.

Figure 6-29 Line Card Cable-Management Bracket



The Cisco 12000 Series Router line cards use cable-management brackets for the following purposes:

- Organizing the network interface cables
- Keeping the network interface cables out of the way
- Positioning connectors at their respective ports on the line card faceplate
- Keeping the cables free of sharp bends (excessive bending in a network interface cable can cause performance degradation)

Note The type of cable-management bracket used by a line card is determined by the line card type and the number of network interface ports on the card faceplate.

To install the line card cable-management bracket, see Figure 6-29 and follow these steps:

Step 1 Attach an ESD-preventive strap to your wrist and connect the leash to the chassis or to another grounded, bare metal surface.

Step 2 Take the line card cable-management bracket from the line card shipping carton.

Step 3 Orient the top of the line card cable-management bracket with the top of the line card faceplate (the end opposite the two four-character alphanumeric displays.)

Step 4 Align the two captive screws on the bracket with the threaded insert holes near the ejector levers on each end of the line card faceplate.

Step 5 Finger-tighten the two captive screws.

Caution Do not overtighten the captive screws; you might strip the threads on the screw or in the insert in the line card faceplate.

Step 6 Use a flat-blade screwdriver to secure the two captive screws.

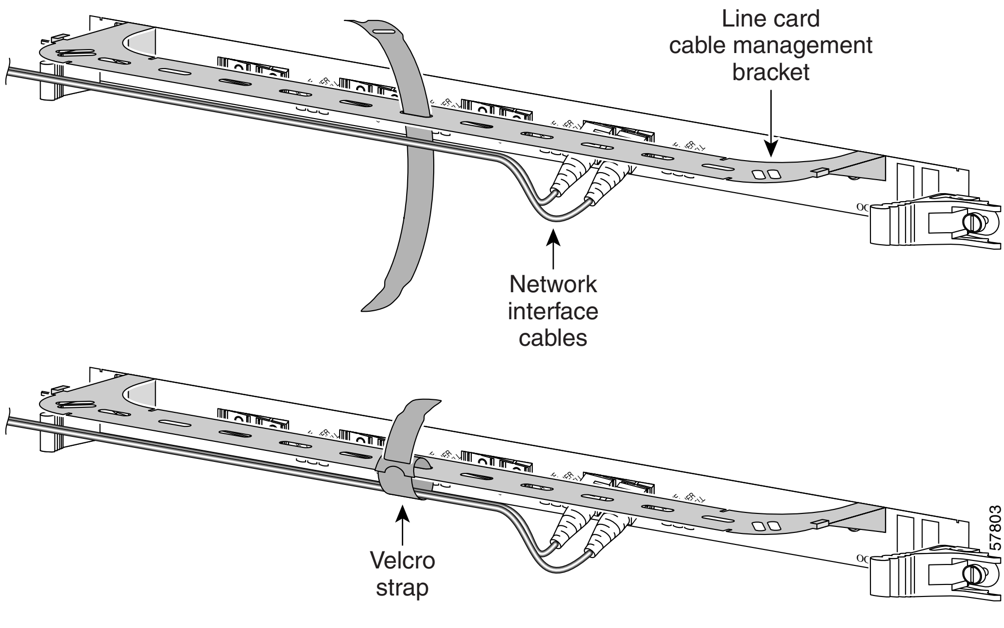
Step 7 Repeat Step 2 through Step 6 for any remaining line cards.

Reconnecting Cables to a Line Card

When you replace an existing line card in the line card and RP card cage, you must reattach the line card cable-management bracket to the line card faceplate and reconnect the network interface cables to the replacement line card as described below.

If you have added a new line card, you must connect the additional network interface cables to the line card and route the cables across the front of the chassis to the vertical chassis cable-management bracket using the line card cable-management bracket as described below and shown in Figure 6-30, which shows a generic cable management bracket and velcro strap assembly.

Figure 6-30 Line Card Cable-Management Brackets with Velcro Straps



To reconnect network interface cables to a line card, follow these steps:

Step 1 Attach an ESD-preventive strap to your wrist and connect the leash to the chassis or to another grounded, bare metal surface.

Step 2 Attach an appropriate number of velcro straps to support the network interface cables, through the slots in the cable-management bracket:

a. Pull the small end of the velcro strap through the slot in the cable-management bracket.

b. Insert the small end of the velcro strap into the slot in the wide end of the velcro strap.

c. Pull the small end through the velcro strap slot to secure it to the cable-management bracket.

Step 3 Proceeding from the left port on the line card to the right port (only on line cards with multiple ports), identify the network interface cable for the line card port and insert the cable connector into the line card port.

Step 4 Align the interface cable with the cable-management bracket.

Step 5 Repeat Step 2 through Step 4 for the remainder of the interface cables for this line card.

Note Carefully adjust the interface cables in the cable-management bracket to prevent any kinks or sharp bends in the interface cables. Kinks and sharp bends can destroy or degrade the ability of the optical fiber to propagate the signal-encoded beam of light accurately from one end of the cable to the other. Also, allow adequate strain relief in the interface cables.

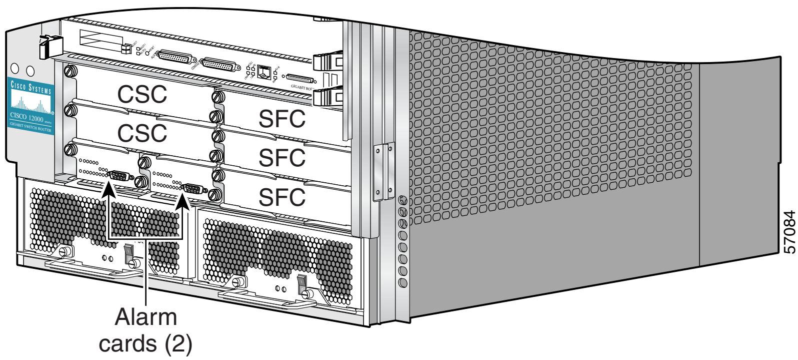
Step 6 Secure the interface cables to the cable-management bracket by wrapping the velcro straps around them. Do not wrap the velcro straps too tightly.

Step 7 Press the velcro strap against itself to secure it.

Removing and Installing a Clock and Scheduler Card, Switch Fabric Card, or Alarm Card

Cisco 12006 and Cisco 12406 routerss are equipped with chassis slots for two CSCs, three SFCs, and two alarm cards. (See Figure 6-31.)

Figure 6-31 CSC, SFC, and Alarm Card Slot Locations



Note The Cisco 12006 Router is based on a 2.5-Gbps switch fabric, where each SFC or CSC provides a 2.5-Gbps full-duplex connection to each line card in the system. The 2.5-Gbps switch fabric consists of the 12006 Advanced Clock and Scheduler Card (product number 12006-CSC=) and the 12006 Advanced Switch Fabric Card (product number 12006-SFC=).

The Cisco 12406 Router is based on a 10-Gbps switch fabric, where each SFC or CSC provides a 10-Gbps full-duplex connection to each line card in the system. The 10-Gbps switch fabric consists of the Clock and Scheduler Card (product number GSR6-CSC=) and the Switch Fabric Card (product number GSR6-SFC=).

You cannot mix 2.5-Gbps switch fabric cards and 10-Gbps switch fabric cards in a chassis. The router will not operate with a mix of switch fabric card types.

Tools and Equipment

You need the following items to remove and replace a CSC, an SFC, or an alarm card:

- ESD-preventive strap
- 3/16-inch flat-blade screwdriver
- Antistatic bag or similar ESD-preventive container

Removing and Installing a Clock and Scheduler Card

A Cisco 12006 or Cisco 12406 Router configured for redundant CSCs will have two CSCs installed in the two CSC slots; a router configured for nonredundant operation will have one CSC installed in one of the CSC slots, and will have a CSC blank filler installed in the second CSC slot. (See Figure 6-31.) Figure 6-32 shows a partially ejected CSC.

Note The CSCs support OIR, so when the router is equipped with two CSCs, you can remove either CSC while the system remains powered up. In a router equipped with only one CSC, you must shut down the router before removing the CSC.

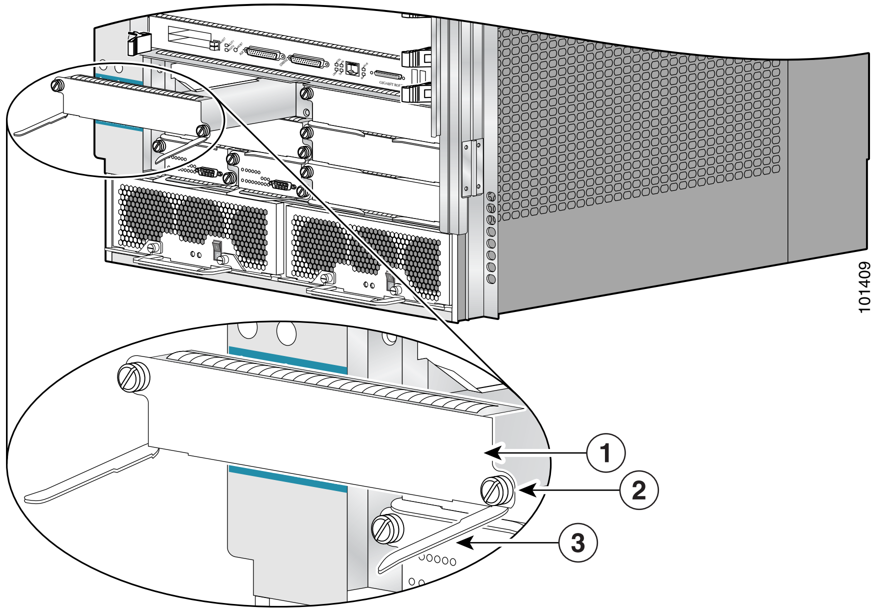
Caution When removing CSCs or CSC blank fillers, remove each component entirely from the chassis and place it in an ESD-safe environment. Do not allow the card or blank to rest partially inserted into the slot, as this will damage the electromagnetic interference (EMI) shielding on the card in the slot directly below.

Caution Two CSCs (redundant configuration) are required to support CSC online insertion and removal (OIR). This allows you to remove and replace a CSC or an SFC while the system remains powered on. If only one CSC is present, do not remove any cards while the system is powered on.

Procedures for removing and installing a CSC are described in these sections:

- Removing a Clock and Scheduler Card, page 6-58
- Installing a Clock and Scheduler Card, page 6-59

Figure 6-32 Removing and Installing a Clock and Scheduler Card



1	CSC	**3**	Ejector lever (2)
2	Captive screw (2)		

Removing a Clock and Scheduler Card

To remove a clock and scheduler card, see Figure 6-32 and follow these steps:

Step 1 Attach an ESD-preventive strap to your wrist and connect the leash to the chassis or to another grounded, bare metal surface.

Step 2 Loosen the two captive screws on each side of the CSC.

Step 3 Grasp the card ejector levers and pivot them away from the CSC faceplate.

Step 4 Slide the CSC halfway out of the slot, then *stop*.

Step 5 Touching only the metal card carrier, use your free hand to support the bottom of the CSC.

Caution When operating your router with a single CSC, the second CSC slot must have a CSC blank filler (MAS-GSR6-CSCBLNK=) installed to ensure electromagnetic compatibility (EMC) compliance, to avoid overheating, and to ensure compliance with regulatory electromagnetic interference (EMI) standards.

Step 6 Slide the card out of the slot and place it directly into an antistatic bag or other ESD-preventive container.

If you plan to return the defective CSC to the factory, repackage it in the shipping container you received with the replacement card.

Installing a Clock and Scheduler Card

To install a clock and scheduler card, see Figure 6-32 and follow these steps:

Step 1 Attach an ESD-preventive strap to your wrist and connect the leash to the chassis or to another grounded, bare metal surface.

Step 2 Remove the CSC from its antistatic bag or ESD-preventive container.

Caution Avoid touching the card circuitry or any connectors.

Step 3 Touching only the metal card carrier, use your free hand to support the bottom of the CSC.

Caution CSC slots are equipped with card alignment grooves on both sides. When you insert a CSC in the slot, make sure you carefully align both edges of the card carrier in the corresponding card slot grooves.

Step 4 Set both edges of the CSC carrier into the card slot carrier alignment grooves on either side of the CSC slot.

Step 5 Pivot the ejector levers away from each other; rotate each ejector lever outward away from the faceplate.

Step 6 Use both thumbs to slide the card carrier into the CSC slot until the ejector levers make contact with the front of the card cage, then *stop*.

Step 7 Pivot the ejector levers toward the faceplate until the connector seats in the backplane.

Caution CSC ejector levers may not fit flush against the CSC faceplate. To ensure that the CSC is properly seated and ensure EMC compliance, tighten the captive screws. Do not overtighten the captive screws; you might strip the threads on the screw or in the insert in the CSC faceplate.

Step 8 Tighten the two captive screws.

Verifying the Installation of the Clock and Scheduler Card

To verify router operation after installing a replacement CSC, visually check the LEDs on the two alarm cards. (See Figure 6-33.) When the system is operating normally, the following LED conditions should be true.

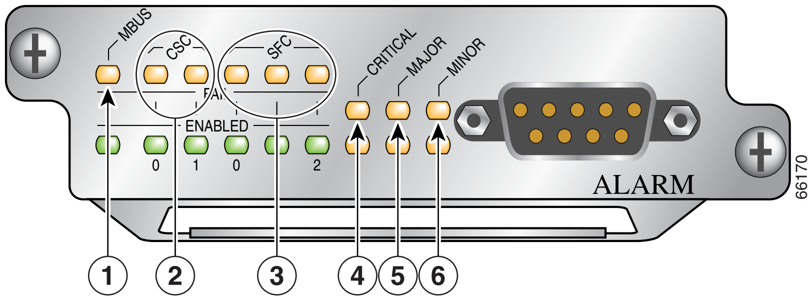
LEDs that normally should be on:

- One MBUS status LED labeled ENABLED
- Two CSC status LEDs labeled ENABLED
- Three SFC status LEDs labeled ENABLED

LEDs that normally should be off:

- One MBUS status LED labeled FAIL
- Two CSC status LEDs labeled FAIL
- Three SFC status LEDs labeled FAIL
- Three router alarm LEDs labeled CRITICAL, MAJOR, MINOR

Figure 6-33 Alarm Card LEDs On/Off Conditions



1	MBus status LED	**4**	Critical alarm LED
2	CSC status LEDs (two)	**5**	Major alarm LED
3	SFC status LEDs (three)	**6**	Minor alarm LED

Removing and Installing a Switch Fabric Card

The three SFCs occupy the three half-width slots on the lower right side of the chassis. (See Figure 6-31.) Figure 6-34 shows a partially-ejected SFC.

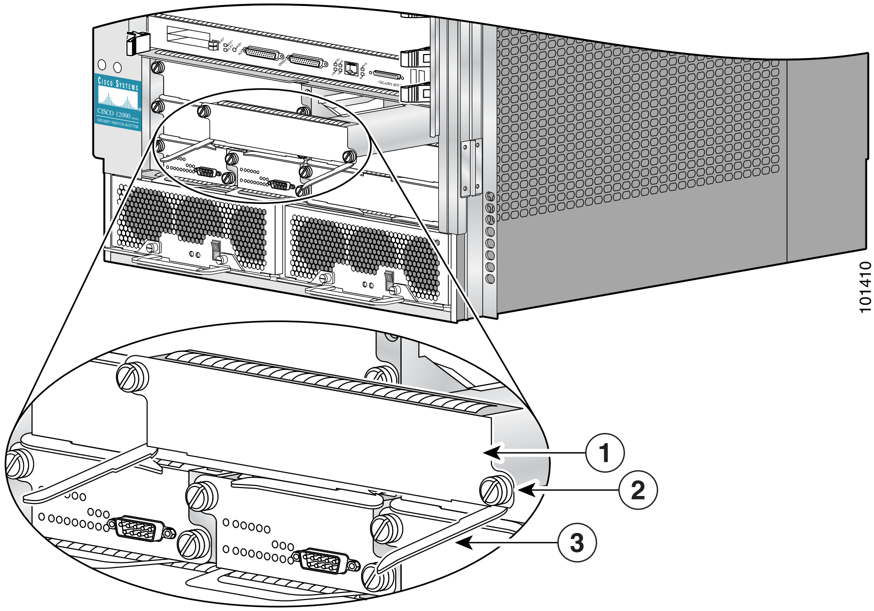
Note Two CSCs (redundant configuration) are required to support CSC online insertion and removal (OIR). This allows you to remove and replace a CSC or an SFC while the system remains powered on. If only one CSC is present, do not remove any cards while the system is powered on.

Caution When removing an SFC, remove the card entirely from the chassis and place it in an ESD-safe environment. Do not allow the card to rest partially inserted into the slot, as this damages the EMI shielding on the card in the slot directly below.

Procedures for removing and installing an SFC are described in these sections:

- Removing a Switch Fabric Card, page 6-62
- Installing a Switch Fabric Card, page 6-63
- Verifying the Installation of the Switch Fabric Card, page 6-64

Figure 6-34 Removing and Installing a Switch Fabric Card



1	SFC	**3**	Ejector lever (2)
2	Captive screw (2)	**–**	–

Removing a Switch Fabric Card

To remove a switch fabric card, see Figure 6-34 and follow these steps:

Step 1 Attach an ESD-preventive strap to your wrist and connect the leash to the chassis or to another grounded, bare metal surface.

Step 2 Loosen the captive screw on each side of the SFC faceplate.

Step 3 Grasp the card ejector levers and pivot them away from the SFC faceplate.

Step 4 Slide the SFC halfway out of the slot, then *stop*.

Step 5 Touching only the metal card carrier, use your free hand to support the bottom of the SFC.

Step 6 Slide the card out of the slot and place it directly into an antistatic bag or other ESD-preventive container.

If you plan to return the defective SFC to the factory, repackage it in the shipping container you received with the replacement card.

Installing a Switch Fabric Card

Switch fabric card captive screws must be tightened to ensure electromagnetic compliance (EMC).

To install an SFC, see Figure 6-34 and follow these steps:

Step 1 Attach an ESD-preventive strap to your wrist and connect the leash to the chassis or to another grounded, bare metal surface.

Step 2 Remove the SFC from its antistatic bag or ESD-preventive container.

Caution Avoid touching the card circuitry or any connectors.

Step 3 Touching only the metal card carrier, use your free hand to support the bottom of the SFC.

Caution SFC slots are equipped with card alignment grooves on both sides. When you insert a SFC in the slot, make sure you carefully align both edges of the card carrier in the corresponding card slot grooves.

Step 4 Set both edges of the SFC carrier into the card slot carrier alignment grooves on either side of the SFC slot.

Step 5 Pivot the ejector levers away from each other; rotate each ejector lever outward away from the faceplate.

Step 6 Use both thumbs to slide the card carrier into the SFC slot until the ejector levers make contact with the front of the card cage, then *stop*.

Step 7 Pivot the ejector levers toward the faceplate until the connector seats in the backplane.

Caution SFC ejector levers may not fit flush against the SFC faceplate. To ensure that the SFC is properly seated and ensure EMC compliance, tighten the captive screws. Do not overtighten the captive screws; you might strip the threads on the screw or in the insert in the chassis.

Step 8 Tighten the captive screw on each side of the SFC faceplate.

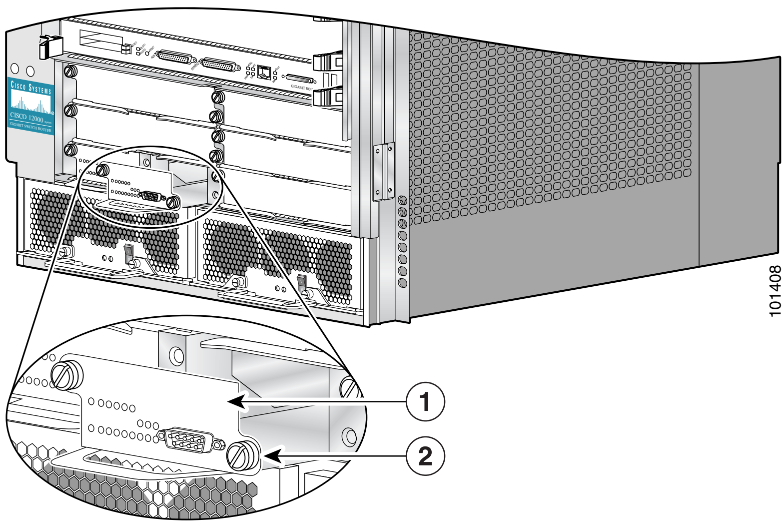
Verifying the Installation of the Switch Fabric Card

To verify router operation after installing a replacement SFC, see the "Verifying the Installation of the Clock and Scheduler Card" section on page 6-60. The description of the LEDs applies equally to checking SFC operation.

Removing and Installing an Alarm Card

The two alarm cards occupy the card slots in the alarm card bay. These slots are located on the bottom left side of the chassis, directly under the clock and scheduler card slots. (See Figure 6-31.) Figure 6-35 shows a partially-ejected alarm card.

Figure 6-35 Removing and Installing an Alarm Card



1	Alarm card	**2**	Captive screw (2)

Note The alarm cards support OIR, so you can remove and install an alarm card while the system remains powered up.

Procedures for removing and installing an alarm card are described in the following sections:

- Removing an Alarm Card, page 6-66
- Installing an Alarm Card, page 6-66
- Verifying the Installation of the Alarm Card, page 6-67

Removing an Alarm Card

To remove an alarm card, see Figure 6-35 and follow these steps:

Step 1 Attach an ESD-preventive strap to your wrist and connect the leash to the chassis or to another grounded, bare metal surface.

Step 2 Loosen the captive screw on each side of the alarm card.

Step 3 Grasp the handle on the front of the alarm card and slide the alarm card halfway out of the slot, then *stop*.

Step 4 Touching only the metal card carrier, use your free hand to support the bottom of the alarm card.

Step 5 Remove the card from the slot and place it directly into an antistatic bag or other ESD-preventive container.

If you plan to return the defective alarm card to the factory, repackage it in the shipping container you received with the replacement card.

Installing an Alarm Card

To install an alarm card, see Figure 6-35 and follow these steps:

Step 1 Attach an ESD-preventive strap to your wrist and connect the leash to the chassis or to another grounded, bare metal surface.

Step 2 Remove the alarm card from its antistatic bag or ESD-preventive container.

Caution Avoid touching the card circuitry or any connectors.

Step 3 Touching only the handle, use your free hand to support the bottom of the alarm card.

Step 4 Slide the alarm card into the alarm card slot until it contacts the backplane, then *stop*.

Step 5 Use both thumbs to push the card carrier into the slot until the alarm card connector seats itself against the backplane connector.

Caution Alarm card captive screws must be tightened to ensure EMC compliance. Do not overtighten the captive screws; you might strip the threads on the screw or in the insert in the alarm card faceplate.

Step 6 Tighten the two captive screws to secure the alarm card in the chassis.

Verifying the Installation of the Alarm Card

To verify router operation after installing a replacement alarm card, see the "Verifying the Installation of the Clock and Scheduler Card" section on page 6-60. The description of the LEDs applies equally to checking alarm card operation.

Removing and Installing the Chassis

Instructions for removing a defective Cisco 12006 or Cisco 12406 Router chassis and installing a replacement chassis are presented in the following sections.

The replacement chassis is an integrated, sheet-metal assembly that includes the following items:

- Six-slot RP and line card cage
- Two-slot clock and scheduler card cage
- Three-slot switch fabric card cage
- Two alarm card slots
- Two air filters
- Two power module bays
- One backplane with connectors

The chassis can be rack mounted or placed on a stable flat surface.

Tools and Equipment

You need the following items to replace a router chassis:

- ESD-preventive strap
- 3/16-inch and 1/4-inch flat-blade screwdrivers
- Number 1 and Number 2 Phillips screwdrivers
- 9/16-inch (14-mm) wrench
- 3/4-inch (19-mm) socket and ratchet wrench
- Vacuum cleaner
- Antistatic bag or similar ESD-preventive container
- Replacement chassis, Part Number: GSR6/120=

Before You Begin

You will need to remove all the components except the air filter from the defective chassis and reinstall them in the replacement chassis. The recommended procedures are as follows:

- The replacement chassis is removed from its shipping packaging and placed temporarily within reach of the rack in which the defective chassis is installed, or near the surface where the defective chassis rests.
- The replacement chassis is connected to the same grounding system as the defective chassis.
- You have prepared a place to set the defective chassis when it is removed from the equipment rack or stable flat surface.
- Components are transferred from the defective chassis to the replacement chassis.
- The replacement chassis (and all the components now installed in it) is inserted into the same equipment rack or on a stable flat surface in place of the defective chassis.

This approach protects the system components—such as line cards, RPs, SFCs, CSCs, and alarm cards—from damage by eliminating the need to store them temporarily outside their card cages, bays, and slots.

Transferring components from one chassis to the other also helps to ensure that the physical configuration of the router is maintained, because each transferred component is installed in the same location in the replacement chassis that it occupied in the defective chassis.

Preparing the Replacement Chassis

Move the replacement chassis near the defective chassis site. Temporarily connect the central office grounding system or interior equipment grounding system to the NEBS supplemental bonding and grounding receptacles on the replacement chassis.

For more information, see the "Supplemental Bonding and Grounding Connections" section on page 3-9.

Preparing the Defective Chassis

To prepare the defective chassis for component removal you must disconnect the power from the PDU and disconnect the RP cables, line card network interface cables, and alarm card cables. These procedures are described in the following sections:

- Disconnecting Power from the Power Distribution Unit, page 6-70
- Disconnecting RP Cables, page 6-70
- Disconnecting Line Card Interface Cables, page 6-71
- Disconnecting Alarm Card Cables, page 6-71

Disconnecting Power from the Power Distribution Unit

Before moving the components from the defective chassis to the replacement chassis, you must first power down the router. Although many of the components in this procedure support OIR, that is, they are hot-swappable, the router must be powered down and completely disconnected from the power sources before you remove the PDU.

Warning **Power down your router.**

To power down the router, see the "Powering Down the Router" section on page 6-2.

Disconnecting RP Cables

Identify and write down each of the RP cable connections on a piece of paper before you disconnect the cables. You must disconnect any cables that are connected to the RP console port, auxiliary port, or to either of the Ethernet ports, RJ-45 or MII (GRP only). After disconnecting the cables, either leave them in the cable management bracket for reuse with the new RP, or move them away from the chassis and place them safely aside.

Disconnecting Line Card Interface Cables

Disconnect the line card network interface cables from each line card as instructed in the “Removing an RP or Line Card” section on page 6-48.

After you disconnect the cables and the line card cable-management bracket from each card, carefully pull the cable bundles out of the way until the cables can be reinstalled on the replacement chassis and reconnected to the line card.

Disconnecting Alarm Card Cables

If there are external alarm device cables connected to the external alarm device connectors on the alarm cards, you must disconnect those cables from the alarm cards as instructed in the “Removing an Alarm Card” section on page 6-66.

After you disconnect the cable from each alarm card, carefully pull the cables out of the way until the cables can be reconnected to the alarm cards in the replacement chassis.

Transferring System Components

The following system components must be transferred between the old and the new chassis:

- RP and line cards
- CSCs, SFCs, and alarm cards
- Power modules (either AC-input power supplies or DC-input PEMs)
- PDU
- Blower module

Transferring these components is discussed below.

Next, the chassis is removed, as explained on page 6-74. Then, the replacement chassis is installed, as explained on page 6-75. Finally, the components that were removed are reconnected, as discussed beginning on page 6-77.

Transferring RP and Line Cards

You must remove the line cards and RP(s) from the line card and RP card cage, then install them in the card cage in the replacement chassis. Card slot blanks must be installed in slots without cards to maintain proper air flow and for EMI performance. RP and line card captive screws must be tightened on the replacement chassis to ensure electromagnetic compliance (EMC).

Caution One edge of the card carrier faceplate is lined with an EMI-preventive gasket consisting of many raised, conductive contacts. Be careful not to damage the gasket contacts, because a damaged card carrier gasket can reduce EMI performance.

Remove each line card in the card cage as instructed in the "Removing an RP or Line Card" section on page 6-48.

Note To match the router's existing software configuration, each card you remove from the defective chassis must be installed in the same slot in the replacement chassis.

Install the line cards as instructed in the "Installing an RP or Line Card" section on page 6-50.

After removing the RP, transfer it to the same card slot in the replacement chassis. Reinstall the RP as instructed in the "Installing an RP or Line Card" section on page 6-50.

Transferring the Clock and Scheduler, Switch Fabric, and Alarm Cards

Remove the two CSCs, three SFCs, and two alarm cards from their slots one at a time and install them in the same slots in the replacement chassis.

Note As you install a CSC, an SFC, or an alarm card in the replacement chassis, tighten the captive screws on the card to ensure electromagnetic compliance (EMC).

Remove each CSC from its slot in the defective chassis as instructed in the "Removing a Clock and Scheduler Card" section on page 6-58. Immediately install the CSC in the same slot of the replacement chassis as instructed in the "Installing a Clock and Scheduler Card" section on page 6-59.

Remove each SFC from its slot as instructed in the "Removing a Switch Fabric Card" section on page 6-62. Immediately install the SFC in the same slot of the replacement chassis as instructed in the "Installing a Switch Fabric Card" section on page 6-63.

Remove each alarm card from its slot in the defective chassis as instructed in the "Removing an Alarm Card" section on page 6-66. Immediately install the alarm card in the same slot of the replacement chassis as instructed in the "Installing an Alarm Card" section on page 6-66.

Transferring the Power Modules

For systems equipped with AC-input power supplies, remove each power supply as instructed in the "Removing and Replacing an AC PEM" section on page 6-18. Immediately install each PEM in the same bay of the replacement chassis.

For systems equipped with DC-input PEMs, remove each PEM as instructed in the "Removing and Replacing a DC PEM" section on page 6-31. Immediately install each PEM in the same bay of the replacement chassis.

Transferring the Blower Module

Remove the blower module from the chassis as instructed in the "Removing and Replacing the Blower Module" section on page 6-9.

Note Set the blower module safely aside temporarily. You will install it on the replacement chassis in a later procedure.

Transferring the Power Distribution Unit

Follow the instructions in the "Removing and Installing the Chassis" section on page 6-68 to remove the PDU from the defective chassis and install it in the replacement chassis.

Detaching the Supplemental Bonding and Grounding Connection

Detach the supplemental bonding and grounding cables from the defective chassis as explained in the "Supplemental Bonding and Grounding Connections" section on page 3-9.

Removing the Chassis

This section contains the following procedures:

- Removing the Chassis from a Tabletop or Flat Surface, page 6-74
- Removing the Chassis from the Equipment Rack, page 6-74

Removing the Chassis from a Tabletop or Flat Surface

Because of the weight and awkwardness of lifting and supporting the chassis, you will need two persons to remove the chassis from a tabletop or other flat surface safely. Each person should review and observe the safe lifting guidelines in the "Lifting Guidelines" section on page 2-5 before attempting to remove the chassis.

To remove the defective chassis from a tabletop or flat surface, follow these steps:

Step 1 Ensure that all cables are disconnected and moved out of the way.

Step 2 With one person positioned on each side of the chassis to lift the weight of the chassis and hold it steady, move the chassis off of the tabletop or flat surface and carry it to the place prepared to store the defective chassis temporarily after it is removed.

Step 3 Set the chassis safely aside.

Removing the Chassis from the Equipment Rack

Before you remove the defective chassis from the equipment rack, examine how the chassis is mounted in the rack:

- Mounted directly against the rack flanges, but sitting on the optional rack-mounting brackets (see Figure 3-1 on page 3-4)

- Mounted directly against the rack flanges
- Mounted using the center-mount bracket kit (see Figure 3-2 on page 3-5)

Because of the weight and awkwardness of lifting and supporting the chassis, you will need three persons to remove the chassis from the rack safely. Each person should review and observe the safe lifting guidelines in the "Lifting Guidelines" section on page 2-5 before attempting to remove the chassis from the rack.

To remove the defective chassis from an equipment rack, follow these steps:

Step 1 Ensure that all cables are disconnected and moved out of the way.

Step 2 Loosen—but do not remove—the screws that secure the chassis to the equipment rack.

Step 3 With one person positioned on each side of the chassis to support the weight of the chassis and hold it steady, have a third person remove the screws that secure the chassis to the equipment rack.

Step 4 Move the chassis out of the rack and carry it to the place prepared to store the defective chassis temporarily after it is removed from the equipment rack.

Step 5 Set the chassis safely aside.

Installing the Replacement Chassis

This section explains the following procedures:

- Installing the Chassis on a Tabletop or Flat Surface, page 6-75
- Installing the Chassis in the Equipment Rack, page 6-76

Installing the Chassis on a Tabletop or Flat Surface

Install the replacement chassis as instructed in the "Installing the Chassis on a Tabletop or Flat Surface" section on page 3-9.

Installing the Chassis in the Equipment Rack

Before removing the chassis from the equipment rack, you determined how the chassis was mounted in the rack:

- Mounted directly against the rack flanges, but sitting on the optional rack-mounting brackets (see Figure 3-1 on page 3-4)
- Mounted directly against the rack flanges
- Mounted using the center-mount bracket kit (see Figure 3-2 on page 3-5)

Use the same mounting arrangement and install the replacement chassis as instructed in the “Installing the Chassis in a Rack” section on page 3-7.

Reattaching the Supplemental Bonding and Grounding Cable

Reattach the bonding and grounding cable lugs to the bonding and grounding receptacles as described in the “Supplemental Bonding and Grounding Connections” section on page 3-9.

Reconnecting Cables to the Replacement Chassis

This section explains the following procedures:

Reconnecting RP Cables

Reconnect the cables to the RP as instructed in the “Connecting RP and Line Card Cables” section on page 3-11.

Reconnecting Alarm Cards Cables

Reconnect the cables to the alarm cards as instructed in the “Connecting Alarm Card Cables” section on page 3-13.

Reconnecting Line Card Network Interface Cables

Reconnect line card network interface cables as described in the "Connecting RP and Line Card Cables" section on page 3-11.

Reconnecting Power to the Router

For AC-powered systems, connect the facility AC power cables to the AC PDU as instructed in the "Connecting to an AC Power Source" section on page 3-29.

For DC-powered systems, connect the facility DC power cables to the DC PDU as instructed in the "Connecting to a DC Power Source" section on page 3-32.

Installing the Blower Module

Install the blower module on the replacement chassis as instructed in "Removing and Replacing the Blower Module" section on page 6-9.

Restarting the Router

Restart the router and verify that it has restarted successfully after replacing the chassis as instructed in the "Power On the Router" section on page 3-35.

Upgrading the RP and Line Card Memory

To upgrade the RP and line card memory, refer to the *Cisco 12000 Series Router Memory Replacement Instructions* publication (Document Number 78-4338-xx). It is available on-line at http://www.cisco.com and on the Cisco CD-ROM.

This publication contains the latest information about memory requirements and replacing memory on the Cisco 12000 Series Router RP and line cards. Consult this publication before replacing memory on your RP or line card, or adding memory to your RP or line card.

Technical Specifications

This appendix provides information and technical specifications for the Cisco 12006 and Cisco 12406 Routers.

Specifications

This section lists the Cisco 12006 and Cisco 12406 Router specifications in these tables:

- For physical specifications, see Table A-1 on page A-2
- For electrical specifications for systems equipped with the AC-input power subsystem, see Table A-2 on page A-3
- For electrical specifications for systems equipped with the DC-input power subsystem, see Table A-3 on page A-4
- For a list of the environmental specifications, see Table A-4 on page A-5

Table A-1 Physical Specifications

Description	Value
Chassis height	18.5 in (46.9 cm)
Chassis width	17.3 in (43.9 cm)
Chassis depth	28.0 in (71.1 cm), including cable-management system
Slot capacity	6 slots
Aggregate switching capacity	Cisco 12006: 30 Gbps Cisco 12406: 120 Gbps
Full-duplex throughput per slot	Cisco 12006: 2.5 Gbps/slot Cisco 12406: 10 Gbps/slot
Physical	Chassis height • 18.5 in. (47.0 cm) Chassis width • 17.3 in. (43.9 cm) • 19 in. (48.24 cm)[1] Chassis depth • 28.0 in. (71.1 cm) • 30.75 in. (78.1 cm)[2] Weight • 140 lb (64 kg)[3] • 213 lb (97.4 kg)[4]
Chassis per rack	Four

1. Including chassis rack-mount flanges and front door width
2. Including cable-management system and front cover
3. Chassis only
4. Chassis fully configured, using all card slots, AC or DC power supplies, and frosted doors and hinges

The electrical specifications and values listed in Table A-2 are for a system equipped with the AC-input power distribution unit (PDU) and AC-input power supply modules.

Table A-2 AC-Input Power Supply Electrical Specifications

Description	Value
Rated input voltage[1]	100–120 VAC nominal (range: 85 to 135 VAC)[2] 200-240 VAC nominal (range: 180-264 VAC) 220–240 VAC (UK)
Rated input line frequency[1]	50/60 Hz nominal (range: 47 to 63 Hz) 50/60 Hz UK
Input current rating[1]	13A @ 200-240 VRMS per line cord (max)
Source AC service requirement[1]	20A North America; 16A international; 13A UK
Nominal output voltage and current	-54.5VDC @ 30A maximum (original series) -54.5VDC @ 36A maximum (enhanced series)
Total AC input power	1708 VA (original series) 2210 VA (enhanced series)
Redundancy	2 AC-input power supply modules are required for 2N redundancy

1. For each AC-input power supply module.
2. Original series only. 110 V AC is not supported on enhanced series.

Caution To ensure that the chassis configuration complies with the required power budgets, use the on-line power calculator. Failure to properly verify the configuration may result in an unpredictable state if one of the power units fails. Contact your local sales representative for assistance.

The electrical specifications and values listed in Table A-3 are for a system equipped with the DC-input PDU and DC-input power entry modules (PEMs).

Table A-3 DC Power Entry Module Electrical Specifications

Description	Value
Rated input voltage[1]	–48 VDC nominal in North America –60 VDC nominal in the European Community (range: –40.5 to –72 VDC) –40 VDC to –72 VDC steady-state input voltage
Input current rating[1]	60A per feed (max)
Source DC service requirement[1]	60A
Nominal output voltage and current	-48VDC @ 40A maximum (original series) -54.5VDC @ 36A maximum (enhanced series)
Total DC input power	1630 VA (original series) 2290 VA (enhanced series)
Redundancy	2 DC-input PEMs are required for 2N redundancy

1. For each DC-input PEM.

Caution To ensure that the chassis configuration complies with the required power budgets, use the on-line power calculator. Failure to properly verify the configuration may result in an unpredictable state if one of the power units fails. Contact your local sales representative for assistance.

Table A-4 Environmental Specifications

Description	Value
Temperature	32° to 104°F (0° to 40°C) operating –4° to 149°F (–20° to 65°C) non-operating
Humidity	10 to 90% noncondensing operating 5 to 95% noncondensing non-operating
Altitude	0 to 10,000 ft. (0 to 3,000 m) operating 0 to 15,000 ft. (0 to 4,570m) non-operating
Heat dissipation	5,828 Btu/hr maximum (AC original series) 8,871 Btu/hr maximum (AC enhanced series) 5,562 Btu/hr maximum (DC original series) 8,871 Btu/hr maximum (DC enhanced series)
Cooling	Facing the router, right-side-to-back cooling
Shock	5 to 500 Hz, 0.5g[1] (0.1 oct/min[2]) operating 5 to 100 Hz, 1g (0.1 oct/min) non-operating 100 to 500 Hz, 15g (0.2 oct/min) 500 to 1,000 Hz, 1.5g (0.2 oct/min)

1. g = Gravity
2. oct/min = Octave per minute

Caution Exhaust from other equipment vented directly into the Cisco 12006 and Cisco 12406 Router air inlet may cause overheating. Install the router so that it is protected from a direct flow of hot air from other equipment.

Alarm Card Alarm Relay Connector Specifications

The alarm card alarm relay connector is a standard DB-9 connector. The relay interface is rated at max 2A, 60V, or 50VA, whichever is greater. The connector pins and their definitions are shown in Table A-5.

Table A-5 Alarm Card Alarm Relay Contact Connector Pinout

Pin	Name	Definition
1	Critical_NO	Critical, normally open contact
2	Critical_C	Critical, common contact
3	Major_NO	Major, normally open contact
4	Minor_NO	Minor, normally open contact
5	Minor_C	Minor, common contact
6	Critical_NC	Critical, normally closed contact
7	Major_NC	Major, normally closed contact
8	Major_C	Major, common contact
9	Minor_NC	Minor, normally closed contact

Router Performance Upgrades and Model Identification

The compliance information label on the side of the chassis also identifies the Cisco 12000 Series Router by its model number. The model number indicates the router is in the Cisco 12000 Series, the maximum switching capacity the router supports, and the number of line card and RP slots in the chassis.

For example, the Cisco 12006 Router features 30 Gbps switching capacity in a 6-slot, 2.5-Gigabit per slot chassis, whereas the Cisco 12406 Router features 120 Gbps switching capacity in a 6-slot, 10-Gigabit per slot chassis. Table A-6 lists the Cisco 12006 and Cisco 12406 Routers and provides model comparison information based on chassis slot counts, maximum switching capacity, and switch fabric type.

Table A-6 Cisco 12006 and Cisco 12406 Router Model Comparison

Model	Chassis Slots	Switching Capacity	Switch Fabric Identification
12406	6	120 Gbps	SFC and CSC
12006	6	30 Gbps	SFC-30/120 and CSC-30/120

On Cisco 12000 Series Routers that support switching capacity increases through switch fabric upgrades, there are some administrative considerations to observe after performing the upgrade and verifying its installation:

- The switch fabric upgrade does not include a new label that identifies the router by the new model number. The compliance label on the router chassis does not change. This could confuse technicians who might service the router in the future. Cisco recommends that the upgrade technician take any required administrative steps to make the new, post-upgrade router identity outwardly obvious.
- If steps are not taken to identify a router with upgraded switch fabric, the alternative methods for identifying an upgraded router are through either Cisco IOS software commands or the Cisco identification labels on the switch fabric cards (SFCs and CSCs) installed in the router. Table A-6 lists the router models and their corresponding switch fabric card identification labels.

INDEX

D

E

I

L

M

N

O

R

S

T

U

V

W